School of Industrial and Information Engineering
Master of Science in Management Engineering

POLITECNICO
MILANO 1863

# Digital Identity in Italy: challenges and opportunities for the adoption in banking, insurance and utility sectors

Supervisor:
Luca Gastaldi

Co-supervisors:
Giorgia Paola Dragoni, Clarissa Falcone

Author:
Enrico Mentasti
900432

Academic Year: 2020-21

# Abstract

*English version*

The impetuous growth of the digital transformation phenomenon, and the global pandemic of Covid-19, radically changed how the world behaves and interacts. The last two years have been characterized by imposed lockdowns and reduced in-person contact. Companies and Governments had to adapt and develop digital solutions to carry out transactions with customers and citizens. This resulted in a critical need to remotely validate identity in a secure, reliable, and simple way. Governments, especially in the European scenario, are running project for national digital identity solutions, appealing both to the public and private sectors. The aim of this study is to understand how the banking, insurance and utility industry are managing the digital identity of their customers. Moreover, what barriers and drivers could affect their attitude for adoption of a national digital identity system. The research was conducted using two units of analysis, the most diffused national digital identity systems of Italy, i.e., SPID and CIE. Fifteen interviews with managers of the private sector have been conducted, verbatim transcribed, and a coding procedure has been performed, extracting concepts consistent with the empirical evidence. For the banking industry, while digital banks are positive towards the two solutions and are running plans for adoption, traditional banks are satisfied with their current identity systems and have concerns regarding regulation, integration and switching costs. Insurance and utility companies are mostly unattracted by the high level of security of CIE and SPID, with concerns regarding user experience. Moreover, the identification process is not critical enough to justify implementation and running costs of the two solutions. A further barrier is represented by mislead communication: many of the interviewed managers, at first, considered SPID and CIE as solutions exclusively dedicated to the public sector.

**Keywords:** identity, digital identity, SPID, CIE, onboarding, authentication

*Italian version*

La crescita inarrestabile del fenomeno della trasformazione digitale e la pandemia di Covid-19, hanno cambiato radicalmente e irreversibilmente i nostri comportamenti e il nostro modo di relazionarci col mondo. Questi ultimi due anni sono stati caratterizzati da diversi lockdown e da una drastica riduzione delle interazioni fisiche tra persone. Sia il settore privato che quello pubblico si sono dovuti adattare, sviluppando soluzioni digitali in modo da operare da remoto con clienti e cittadini. Di conseguenza, è cresciuta la necessità di verificare le identità di cittadini e utenti a distanza, in maniera sicura, semplice e affidabile. I Governi, specialmente quelli europei, hanno avviato progetti di identità digitali nazionali, rivolti sia al settore pubblico che a quello privato. Lo scopo di questa ricerca è capire come i settori bancario, assicurativo e utility gestiscono le identità digitali dei propri clienti. Inoltre, quali barriere e stimoli possono incidere sulla propensione verso l'adozione di un sistema nazionale di identità digitale. La ricerca è stata condotta utilizzando due unità di analisi: i due sistemi nazionali di identità digitale più diffusi in Italia, SPID e CIE. Sono state condotte interviste con dirigenti e manager del settore privato, successivamente trascritte, ed è stata effettuata una procedura di codifica, estraendo concetti chiave coerenti con l'evidenza empirica. Riguardo il settore bancario, le banche digitali sono interessate alle due soluzioni e stanno conducendo progetti per l'adozione. Le banche tradizionali, invece, sono soddisfatte dei loro sistemi di identità attuali e hanno preoccupazioni in materia di normativa, integrazione e costi di adozione. Le aziende del ramo energetico e assicurativo sono per lo più indifferenti verso l'alta sicurezza propria di SPID e CIE, con preoccupazioni in materia di esperienza utente. Inoltre, il processo di identificazione non è altamente critico, e quindi non giustifica i costi di adozione e operativi delle due soluzioni. Una ulteriore barriera riguarda un problema di comunicazione: molti dei dirigenti intervistati in precedenza credevano che SPID e CIE fossero due soluzioni legate solamente alla Pubblica Amministrazione.

**Parole chiave:** identità, identità digitale, SPID, CIE, onboarding, autenticazione

# Contents

# EXECUTIVE SUMMARY

## Introduction

The digital transformation is shaking the world from a social, political, and economic point of view. As the years go by, more and more transactions are conducted online.

Everyday people around the world go through onboarding and authentication processes to be able to access services, and most of these require a basic form of digital identity, as it happens for social networks and e-commerce platforms. However, the digitalization process is also affecting those sectors where a self-asserted identification is not sufficient and a proof for identity is necessary to conduct transactions.

A key dimension to understand the potentiality and destination of use of a digital identity system is the "Level of Assurance" (LOA). The World Economic Forum[1] states that the LOA in an identity transaction is "the degree of certainty that the transacting parties have in the veracity of the identity being presented." The Level of Assurance is the ability to determine whether a claim on a particular identity made by some person or entity can be trusted to be the claimant's true identity.

The financial sector, particularly, is passing through a process of significant transformation. Many actors of the banking industry want to deliver pure digital offerings, but the process of identifying users, that is fundamental to be managed at a high LOA, consistently forces them to use physical channels.

[1] World Economic Forum, "Identity in a Digital World: A new chapter in the social contract" (2018)

At the same time, Governments have started carrying out national digital identity programs to enable interactions at high LOA between citizens, Public Administration and beyond.

The global pandemic of Covid-19 furtherly increased the necessity to perform online transaction. Those organizations that had strong digital identity could maintain at least some continuity of service delivery by shifting from physical to remote channels, establishing habits and expectations in citizens that will remain and condition the post-pandemic scenario.

Particularly, the European Union is moving towards a communitarian digital identity ecosystem. Both the eIDAS regulation[2], published in 2014, and its revision proposal of June 2021, are enforcing Member States into developing national digital identity solutions. The objective of this project is to allow interactions between citizens and both private and public organizations across the European Union.

The growing importance of digital identity drowned the attention of the scientific community around the topic, but many fronts remain open. Specifically, the academic context lacks a comprehensive framework for guidelines and a roadmap on how to effectively populate the ecosystem, especially referring to the private sector. It is not clear which elements may constitute a sufficient advantage for private service providers such as to originate a natural willingness to enter the ecosystem.

To explore this gap, this thesis examines the case of SPID and CIE, and how they relate to companies of the banking, insurance, and utility industries.

# Methodology

**SPID and CIE as units of analysis**

SPID or Sistema Pubblico di Identità Digitale, is the most widespread national digital identity system in Italy. By October 2021 it counts 26.1 million of releases. It

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

was initially conceived in 2014 by the National Agency for Digitalisation (Agenzia per l'Italia Digitale, in Italian; hereafter AgID), a public agency established by the Italian government in 2012 responsible for the digital transformation of the Public Administration in Italy.

AgID oversees the regulatory and strategic development of the platform, in partnership with nine Identity Providers (IdPs), which are public and private organizations, and are in charge for the registration and the issuance of SPID.

SPID 9 IdPs are: Aruba, Infocert, In.Te.S.A., Lepida, Namirial, Poste Italiane, Sielte, Register, TI Trust Technologies.

SPID is available in 3 levels. To the higher level corresponds a higher level of LOA, and a higher fee to be paid by the SP to the IdP.

CIE or Carta d'Identità Elettronica (Electronic Identity Card), is the national card-based digital identity system in Italy. It is the smart equivalent of the traditional identity card and acts both as a physical document and a digital identity solution; it was first released in 2016, it counts 24.7 million of releases by October 2021 and it is provided with a chip capable of exchanging information through NFC technology.

CIE architecture is centralised, it is issued by the Ministry of the Interior, and the app is released by the Italian Bureau of Engraving and Printing (Istituto Poligrafico Zecca dello Stato).

To complete the description of the ecosystems, it is necessary to consider also the side of the Service Providers (SPs). At the time of October 2021, SPID presents 16,076 public SPs and 59 private SPs, while CIE has 1,790 public SPs and 3 private SPs.

**Data analysis methodology**

After a deep analysis of the existing literature on the digital identity topic, and after identifying the most suitable analysis units in SPID and CIE, the data collection phase began. A total of 15 interviews with an average duration of 45 minutes have been performed between October 2021 and January 2022 to managers of 15 different companies, comprehending 6 banking institutions, 5 insurance companies and 4 organizations operating in the utility field.

After having transcribed verbatim each interview, a coding procedure was initiated. Data analysis has been conducted following the Gioia Methodology, a holistic approach to inductive concept development (Gioia et al., 2012), that consists of a coding procedure of examining transcribed data, capturing, and categorizing notions that describe or explain a phenomenon into variables identified as "concepts".

As the interviews were progressing, the processes of transcribing data, coding and analysing were carried out in parallel, as suggested by Glaser and Strauss (1967), obtaining intermediate insights and ideas. As Eisenhardt (1989) stated, overlapping data analysis allowed a flexible data collection and enabled the possibility of making adjustments as the research progressed. In particular, this research took advantage from the addition of questions to the initial interview protocol.

The description of results in chapter 4 is structured according to both the intra-sectoral and infra-sectoral nature of the research. Firstly, industries are analysed separately; then, in the second half of the chapter, general findings resulting from a comparative analysis of the three sectors are presented.

## Empirical analysis

This chapter presents the results of a research aimed to understand barriers, drivers, and opportunities for the implementation of SPID and CIE in the private sector.

**Banking sector**

The banking industry is highly regulated, and a high LOA is required for most interactions with customers. Two different categories of banks can be identified: digital and traditional banks.

Digital banks act as forerunners, driven by their need of remotely identifying users. Two out of three actors interviewed adopted SPID for onboarding, and they registered greatly positive results, both in terms of security, cost, and user experience, leading to increased trust towards national digital identity systems and encouraging the implementation of CIE.

Traditional banks are a step behind: their customer base is not as digital oriented, and the number of customers recognized at a distance is limited. Even if none of the actors have already implemented SPID or CIE, they look at the theme with increasing interest, and the national solutions are observed with attention.

Summarizing, while CIE and SPID are solutions that address a real, strategic, and immediate need of digital banks, traditional banks are staying a step behind. Currently, innovating online onboarding is not a priority and, in such a regulated industry, every process involving identity is important and costly.

**Insurance sector**

The insurance industry presents two different categories: online insurances, that base their business on selling car policies, and traditional insurances, that look for a deeper understanding of their customers to sell multiple insurance products.

For online insurance companies there is no reason to invest into SPID for a higher LOA when it is not required for the process, resulting in a very low interest and adoption inclination.

Most of traditional insurances do not offer an online onboarding procedure, mainly because their entire business model is based on agents and their ability to relate with customers.

The main barriers depend on the tradeoff between value and costs. The insurance industry results difficult to attack, without either improving the value proposition of SPID and CIE, or by restructuring integration and utilization costs of the two systems.

**Utility sector**

The utility industry presents a discrete propension toward the adoption of external digital identity systems, supported by a certain degree of flexibility in terms of regulation of the market. However, the perceived value of SPID and CIE remains notional, and struggles to trigger an action for adoption. In fact, this industry does not require a high LOA identification and, moreover, the rate of use of the personal area is very low.

**CIE is a step behind**

The biggest insight that comes as a result of this research is that SPID appears significantly more appealing to the private sector compared to CIE.

Several reasons have been identified:

- SPID is more widespread
- A network of IdPs support SPID
- CIE NFC technology might constitute a barrier for authentication purposes

**The authentication problem**

None of the interviewed companies considered using SPID for authentication purposes.

While for the banking industry an adoption of SPID and CIE would not deliver any advantage compared to the sophisticated current systems in use, the insurance and utility companies are held back by a limited use of the personal area by customers.

**Suggested evolution: enrich the set of identity data**

Managers suggested that an enrichment of data obtainable through SPID could enhance its value proposition, either by expanding the set of data a user can store into its digital identity, or by using SPID as a proof of consent to share data across firms.

## Conclusion

The objective of this chapter is to present solutions and guidelines on how to successfully enable the adoption of national digital identity systems among private service providers.

**Enhancing cost-benefit tradeoff**

Most barriers of the insurance and utility industries are related to the cost-benefit tradeoff not favouring SPID and CIE adoption.

Benefits wise, managers themselves identified the enrichment of attributes accessible through the national digital identity systems as the most interesting paths to enhance the value of SPID and CIE.

Cost wise, insurance and utility companies would be interested in the implementation of SPID at level 1, that does not require a multi-factor authentication and is cheaper, if compared to SPID of level 2 and 3.

Nevertheless, costs for the implementation of SPID and fees for its usage appear to be too expensive for firms to inspire adoption, and some actions should be taken in these regards, with two non-mutually exclusive possibilities:

- Facilitate the implementation of SPID.
- Reduce or nullify the fees for level 1 SPID usage.

**Solving regulation and integration concerns**

Actors of the banking industry showed concerns on SPID and CIE from a regulatory perspective, and regarding the division of responsibility between SP and IdP in case of frauds during the recognition process. A clear stance on the validity of these solution for identification in the banking industry, and as well the definition of a clear regulatory framework, are necessary to address these uncertainties and remove these barriers.

A further theme that emerged is about a lack of standardization. An action from the regulatory body to ensure standardization would be able to take out this barrier.

**The role of communication**

Communication is key in obtaining a wide diffusion for digital identity solutions. Several managers have reported how in the first place SPID and CIE were perceived as solutions exclusively meant for the public sector. Targeted communication in these regards could greatly impact the perception of SPID and CIE among both firms and citizens.

Moreover, currently CIE is perceived as a substitutive solution of SPID, rather than complementary. Communication on alternative use-cases for CIE and on its ease of use could partially or totally fill the gap between the two solutions in exam.

# 1 INTRODUCTION

Digital is changing the world. The digital transformation has had a great impact on the human society, reshaping the way people, companies and governments interact, produce, and consume value. As digital connectivity and the online activities of individuals grow, our digital identities are increasingly embedded in everything we do in our daily lives.

## 1.1. The context of digital identity

Compared to just a few years ago, digital identity is now routinely required for transactions. The need of reducing costs and increase efficiency moved both private and public organizations to online services. Indeed, as Sullivan (2013) pointed out, as dealings conducted in person are replaced by dealings conducted without a history of personal acquaintance, without face-to-face interaction, and often without any human contact, the requirement to use digital identity for transactions has increased.

In fact, a proof for identity is necessary to conduct all those transactions where a self-asserted identity is not sufficient, and these interactions are becoming more and more frequent on the digital economy.

Every day, citizens around the world go through authentication processes that give others confidence in who they claim to be to access a service, and those services are

accessed through account logins or biometrics, such as fingerprint or facial recognition.

As described in a Deloitte report[3], with data flowing freely within an organization and the disappearing boundaries between networks, identity has become the crucial point to manage, control, and govern access to data and applications.

Moreover, digitalization evolved the concept of identity, that is not any more exclusively bounded to humans but can include identities of computers, mobile phones, devices, services, etc.

The global pandemic of Covid 19 has furtherly increased the need to perform remote transactions, drawing attention on the "fundamental role that digital ID and government-to-person payment ecosystems can play in helping a country to deliver services and social assistance to its people rapidly, effectively and responsibly" (World Bank Group, 2021[4]).

This process of digitalization, and thus the need for digital identity, is affecting both the private and public sectors, with companies and government that are empowering their capability of offering online services.

The financial sector, particularly, is passing through a process of significant transformation: old identity systems are limiting Fintech innovation and well as secure and efficient service delivery in financial services and society more broadly. Many actors of the banking industry want to deliver pure digital offerings, but the process of identifying users, that is fundamental to be precise and secure, consistently forces them to use physical channels (World Economic Forum, 2016[5]).

At the same time, Governments have started carrying out national digital identity programs to enable interactions between citizens and Public Administration and beyond.

---

[3] Deloitte, "Digital Identity" (2020) https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-DigitalIdentitiy-24sep-noexp.pdf

[4] World Bank Group, "ID4D & G2Px annual report 2021" (2021)

[5] World Economic Forum, "A Blueprint for Digital Identity" (2016)

As asserted by the World Bank Group (2016), digital identity could be the answer to the identity gap that affects emerging countries. About 1 billion of people in the world lack any form of recognized identification, either physical or digital. Given the falling costs of technologies like smartphones and scanners, rising access to internet infrastructure, and the shift online of more consumer and government services, identification methods that can be used securely over digital channels will be more important than ever to facilitate economic transactions, social interactions, and political involvement.

Covid-19 highlighted the potentiality of digital identity. Those nations that had strong digital identity, digital databases, and digital payments pre-pandemic were able to leverage these to target new social assistance beneficiaries at a higher scale and make payments more efficiently and safely through digital methods (World Bank Group, 2021). These countries could maintain at least some continuity of service delivery by shifting from physical to remote channels, establishing habits and expectations in citizens that will remain and condition the post-pandemic scenario.

## 1.2. Digital identity in the European Union

Shifting towards the European scenario, in 2014 the European Commission has developed the eIDAS[6], a regulation on electronic identification and trust services for electronic transaction for the European internal market. eIDAS is comprehensive of a framework for a legally recognized digital identity, defining 9 principles to be observed, being: user choice, privacy, interoperability and security, trust, convenience, user consent and control proportionality, counterpart knowledge and global scalability.

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

However, the eIDAS Regulation did not establish any obligation for Member States to develop a national digital identity system and to grant interoperability across Europe, leading to fragmentation[7].

Therefore, the European digital identity panorama resulted to be highly variated, in terms of adopted technologies, involved institutions and diffusion.

On 3rd June 2021, the Commission published its proposal on a European digital identity framework based on the revision of the current one[8], addressing shortcomings in eIDAS by improving the effectiveness of the framework and, most importantly, extending its benefits to the private sector.

Member States will offer digital wallets, thanks to the which citizens and businesses will be able to link various aspects of their national digital identities. These may be provided by public authorities or the private sector if they are recognized by the Member States. Consumers should be granted full control of the data they share, without having to use private platforms to access online services.

## 1.3. Thesis presentation

Having described the context on which this thesis project lays in, it becomes fundamental understanding what are the different characteristics embodied in a digital identity, and how those can affect its impact in the society. Moreover, the eIDAS revision made clear that a comprehensive digital identity cannot be reached without involving the private sector in the ecosystem, along with Public Administrations and citizens.

---

[7] European Parliament (2021) Updating the European digital identity framework https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)698772#:~:text=On%203%20June%202021%2C%20the,do%20so%20across%20EU%20borders.

[8] European Commission (2021). Proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.
URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281)

Specifically, this thesis project aims to understand what factors affect the willingness of private companies to join national digital identity systems, with a focus on the Italian scenario.

To achieve these goals, this work has been structured in:

- Chapter 2, **Literature**, is a broad research on the Digital identity topic, gathered though articles, reports and books. The literature gap and research questions are presented.
- Chapter 3, **Methodology**, describes the case of SPID and CIE and the methodology used to conduct the empirical analysis.
- Chapter 4, **Empirical Analysis**, presents the empirical evidences collected during the research, enriching them with quotes directly extracted from the salient points of the interviews.
- Chapter 5, **Conclusion**, elaborates the findings presented in the Results, with solutions and possible routes to be followed to answer the research question.

# 2 LITERATURE REVIEW

## 2.1. The digital identity

Identity is a conceptually complex term. It has been defined in different ways and contexts over the years. "At a basic level, we can say that identity, in general, is any set of characteristics that define a person and can be used to uniquely identify that person" (BBVA, 2018[9]).

Identity is "the set of all attributes of an entity, whether it's a human, a business or an object and help to differentiate between each other" (Mohamed and Samion, 2020), and "one or more attributes which are applicable to this particular subject or object" (Rasouli and Valmohammadi, 2019).

Ben Ayed (2014) defined identity as "a set of qualities and characteristics, by which an entity can be defined, distinguished and recognized in comparison to other entities".

As a consequence, digital identity would be the digital version of a person's physical identity, the digital representation of the individual. There is a significant number of digital identity definitions.

For Mohamed and Samion (2020) "Digital identity corresponds to the electronic information associated with an individual in a particular identity system."

[9] BBVA Research, "Digital Identity: the current state of affairs" (2018)

The World Bank Group[10], defined digital identity as "a set of electronically captured and stored attributes and/or credentials that uniquely identify a person".

Bertino at al. (2006) underlines the non-exclusively human nature of digital identity "digital identity is a digital representation of data on a person, organization, or object".

McKinsey[11] distinguishes identification by identity: "identification is the means by which we prove we are who we say we are. This is distinct from identity, which is an individual's unique set of attributes. Identification provides a mechanism to authenticate identity". The digital identity allows individuals to be uniquely identified over digital channels and is used for electronic transactions. (World Economic Forum, 2018[12]).

The Digital Identity Observatory of Politecnico di Milano gives a broad and extensive definition: "digital identity is a collection of data that allows to univocally identify a person, a company or an object, which are digitally gathered, memorized and shared inside an ecosystem of factors and through enabling technologies, and able to grant access to value added digital services."

## 2.2. Towards digital identity

With customer and citizens interaction are moving from physical to online, social and mobile channels, firms and governments are driven to develop new capabilities that will enable smooth transactions in a digital environment.

[10] World Bank Group, "Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation" (2016)
[11] McKinsey, "Digital identification: A key to inclusive growth" (2019)
[12] World Economic Forum, "Identity in a Digital World: A new chapter in the social contract" (2018)

### 2.2.1. Trends

The BBVA research of 2018[13] identified the main drivers behind the development of digital identity systems, with a classification split into user behaviour and technology growth:

- New user behaviour.
    - Rising users' expectation: consumers are not happy with passwords and prefer to use a single identity instead of changing continuously their credentials.
    - Need for trust: the more reliable a digital identity is, the more complex transactions will a user be allowed to perform.
    - Increased concerns on privacy: if customers do not feel that their data are protected, they will not transact online.
- Rise of exponential technology.
    - Big Data: companies have the ability to gather, classify and store vast amount of information.
    - Biometrics: This technology bring both user experience and security improvements.
    - Artificial Intelligence (AI) and Machine learning (ML): Smart automated machines are helping companies to identify suspicious activities.
    - Distributed Ledger Technology: Blockchain could allow the sharing of sensitive data without compromising private information.
    - Diminishing costs: Technology is getting cheaper, and digital identity systems are cheaper to run than physical ones.

[13] BBVA Research, "Digital Identity: the current state of affairs" (2018)

### 2.2.2. Benefits

Digital identity facilitates the interaction of individuals with businesses and governments, impacting positively both on the user and service provider side (McKinsey, 2019). The McKinsey report[14] analysed and identified benefits developed by an increasing digitalisation of identities, both for private and public institutions:

- **Time and cost savings**: High assurance digital identity for registration could cut off 90% of the time spent on onboarding; on the user side, a digital identity reduces drastically the need for travel, positively affecting customer experience and resources.
- **Reduced fraud:** Digital identity can help reduce fraud in a wide range of transactions; theft of identity becomes much harder to happen if a trusted, high assurance, unique identity, is used for transactions.
- **Increased sale of goods and services**: Digital onboarding and digital transactions enables commerce and services fruition.
- **Greater employment and labour productivity**: Digital identity can expand and improve talent matching; businesses could more rapidly fill open positions and find the right employees for a given position, leading to higher productivity.
- **Increased tax collection**: Greater economy efficiency and revenue could positively impact the tax base and lead to a more effective tax collection.

## 2.3. Digital and physical

Digital and physical identity are two distinct and connected concepts. To physically identify an individual, proximity and presence of the involved parties is needed in

[14] McKinsey, "Digital identification: A key to inclusive growth" (2019)

a digital identity system. The Digital Identity Observatory of Politecnico di Milano has identified the differences between digital and physical identity in four characteristics: proliferation, validity, ecosystem, and dynamicity.

**Proliferation:** An individual can own a few digital identity tools, mostly connected to a physical document as a passport or an ID-card. The digital world is characterised by numerous systems and platforms that enable the creation of an account and, subsequently, of an ID, as in the case of Socials and e-Commerce platforms.

**Validity:** Physical IDs are broadly recognized in national – and often international – territory, while digital identity is recognized only by those actors that decide to adhere to the Identity system.

**Ecosystem:** For a physical ID the releasing entity does not take part in the further uses and exhibitions of the document. In a digital system at each authentication an interchange of data happens between – at least - the identity provider, the service provider and the user; the ecosystem is deeply connected, and many actors are involved at each iteration.

**Dynamicity:** Physical identities have a static set of data that does not change along the lifecycle of the document. Data in Digital Identities, on the other hand, is potentially very dynamic, characterised by a highly frequency of updates and by the possibility to add new information to a digital profile.

The World Economic Forum[15] identified three inner improvements that differentiate physical and digital system.

- **From Document based to Digital based**

  Proof of physical identity is based on the possession and *de visu* recognition, and is attached to a physical document which suffers wear of time, while digital identity can be protected by damage, tampering, loss and theft.

[15] World Economic Forum, "A Blueprint for Digital Identity" (2016)

- **From Siloed to Interconnected**

  Physical documents are held in discrete places and cannot be aggregated, while digital identity permits communication and transaction in a digital format.

- **From Inflexible to Flexible**

  Data and information in a document are limited and cannot be adapted to transaction requirement, while digital identity can adapt to the transaction requirements and disclose only the necessary information.

Concluding, physical identity was designed to enable face to face transactions among entities, while digital identity enables transaction in a digital world and can provide added value and improvements to the involved actors.

## 2.4. A good digital identity

The report from McKinsey[16] identified the requisites and characteristics of a good digital identity:

- Is verified and authenticated to a high degree of assurance:

  High-assurance digital identity meets both government and private-sector institutions' standards for initial registration and subsequent acceptance for a multitude of important civic and economic uses; a high level of assurance can be achieved through the use of a wide range of credentials and technologies.

- Is unique:

  With a unique digital ID, an individual has only one identity within a system, and every system identity corresponds to only one individual. This is not the case of social and eCommerce ID.

[16] McKinsey, "Digital identification: A key to inclusive growth" (2019)

- Is established with individual consent:

  Meaning that the user is fully aware of what data will be captured and how those data will be used.

- Protects user privacy and ensures control over personal data:

  Privacy and control of data are key principles of modern digital identity systems.

The community of the World Economic Forum[17], in 2018, identified five elements that a good digital identity must satisfy:

1. Fit for purpose – A good digital identity offers a reliable way for individuals to build trust in who they claim to be, and to exercise their rights to carry out digital interactions.
2. Inclusive – An inclusive digital identity enables anyone who needs it to establish and use a digital identity, free from the risk of discrimination based on their identity related data.
3. Useful – A useful digital identity offers access to a wide range of useful services and interactions and is easy to establish and use. At present, many digital identities have onerous requirements and limited uses.
4. Offers choice – Individuals have choice when they can see how systems use their data and are empowered to choose what data they share for which interaction, with whom, and for how long.
5. Secure – Security includes protecting individuals, organizations, devices and infrastructure from identity theft, unauthorized data sharing and human rights violations.

[17] World Economic Forum, "Identity in a Digital World: A new chapter in the social contract" (2018)

## 2.5. Level of Assurance

A key dimension to understand the potentiality of the use of digital identity is the "Level of Assurance", determined by the degree of reliability of identification and authentication of the user.

The Level of Assurance (LOA) is the ability to determine that a claim to a particular identity made by some person or entity can be trusted to actually be the claimant's "true" identity.

The World Economic Forum (2016) states that the LOA in an identity transaction is "the degree of certainty that the transacting parties have in the veracity of the identity being presented."

A high LOA brings confidence that a person is who she claims to be, it depends on the strength of the identification and authentication processes, and is critical to access control and reducing identity theft.

A high LOA is per se an enabling factor for a digital identity system, since services at high criticalness, such as financial and sanitary transaction, must face high risks and need massive security mechanism.

In these situations, individuals must provide more proofs of our real attributes and what is really important is the validation that others (identity providers or validators) do of the attributes that are shared to prove identity.

For this reason, identity providers with a high level of assurance, like public authorities or financial institutions, are supposed to be the leaders of the future ID market (BBVA, 2018).

It is important to note that ecosystems' actors always face a cost-benefit tradeoff in seeking to achieve higher LOAs:

- economically, since service providers face a tradeoff between the perceived risk of a transaction versus the cost of authenticating that transaction.
- experience-wise, since a high LOA requires intensive onboarding and strong authentication, resulting in processes that can be cumbersome for the user.

For example, a webcam recognition where a user must communicate a passphrase to an operator will incur in higher costs and less user experience if compared to a self-declaration registration, but at the same time providing a high LOA and lower risk in future transactions.

The National Institute of Standards and Technology (NIST[18]) recommends four LOA levels, with level 4 being the strongest and level 1 the weakest. Some SPs may wish to grant a user different access permissions based on the LOA during the current session. For example, a user can be allowed to access and read some content with a LOA of 1 and can modify contents with a LOA of 4 (Chadwick 2009).

As the level of assurance becomes more intense, a higher degree of veracity is required due to confidence being crucial in trade relations (BBVA research, 2018).

Veracity is a concept deeply linked to identity and LOA. An IBM report[19] from 2012 describes veracity as "data uncertainty", referring to the ability of "managing the reliability and predictability of inherently imprecise data types". Veracity has to do with managing "data in doubt" and relates it to "uncertainty due to data inconsistency, incompleteness, ambiguities, and deception".

## 2.6. Pillars

The Digital Identity Observatory of Politecnico di Milano, through their study and research on different identity systems, have identified four key dimensions of digital identity: identity data, accessible services, ecosystem, and technologies.

[18] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
[19] IBM Institute for Business Value (2012) "How innovative enterprises in the midmarket extract value from uncertain data

### 2.6.1. Identity Data

Data are an inner element of a digital identity; they define who an individual is and what he can do. They can be divided in:

- **Static data,** proper of an individual, usually do not change in time and comprehend personal information, biometrics, and certificates.
- **Dynamic data**, gathered through interactions and transaction of the user in the ecosystem, such as financial or sanitary information.

To determine the reliability of data, in a given digital identity system, it is important to esteem the LOA.

### 2.6.2. Accessible services

The main scope of digital identity is to grant users the access to services and operate transactions.

The service world is highly varied, there are services with a low level of criticalness (e.g., social networks), and thus require a low level of assurance, and services at medium-high, like financial and sanitary services, that if compromised can considerably affect users' welfare.

Accordingly, individual can access a social network platform through a relatively unsecure authentication method, usually username and password, while financial services require a much more secure multifactor authentication and make use of complex anti-fraud mechanisms.

### 2.6.3. Ecosystem

The ecosystem is the network of entities involved in the digital identity system, composed by the actors and their role in a Digital Identity System.

According to Cao and Yang (2010), the three core components, or roles, for an identity management system, are:

- **Users,** that are the beneficiary of the service.
- **Identity Providers (IdPs)**, being the entities holding the attributes.
- **Service Providers (SPs)**, that accept the digital identity provided by IDPs and provide services to users.

Different actors can embody one or more roles; how these roles are distributed and the relations between the actors can generate various configurations of Digital Identity systems, described in the "Archetypes" chapter of this literature review.

### 2.6.4. Technologies

Technologies are a key element for the development and diffusion of digital identity systems.

To better understand how different technologies can impact diverse areas of a digital identity, the Observatory established a classification in three categories:

- Architectural technologies, as blockchain and cloud platforms, which affect the constitution and architecture of the system.
- Integrational technologies, such as standard protocols and API management systems.
- Process technologies, such as biometrics recognition devices and machine learning, which relate to the front-end interaction with the final user and can positively affect user experience and security.

## 2.7. Attributes

"Identity is the total set of an entity attributes" (World Economic Forum, 2016). These attributes enable entities to participate in transaction by proving to their counterparty that they have the specific requirements for that transaction.

While it is true that all the identity attributes are personal data, personal data becomes identity attribute only if combined with other elements: for instance, the address is a piece of personal data, but several persons can have the same address (BBVA, 2018).

All the information required to identify any entity is a collection of attributes which can be persistent such as the date of the birth of an individual, temporary (e.g., address) or long-lived (e.g., social security number) (Dib and Toumi, 2020).

In 2008, Wilton designed a model to clarify how the different type of identity data relate to the concept of credential, named "The Onion Model" (Figure 2.1).

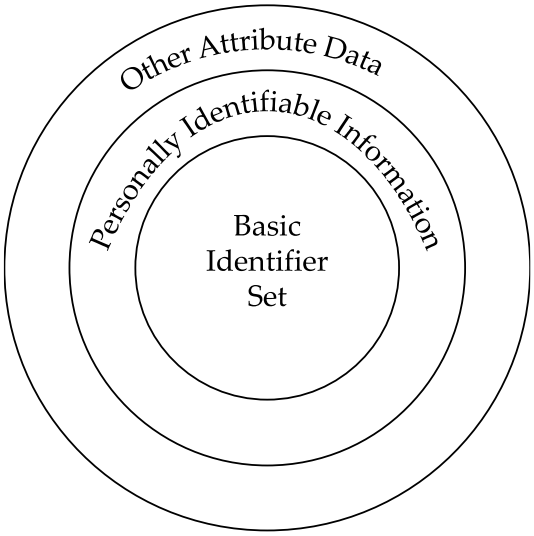



Figure 2.1 - The Onion Model (Wilton, 2008)

Basic Identifier Set is the minimum set of data items necessary to establish a uniqueness of a given person, typically it consists of information such as name, gender, date, and place of birth.

The middle ring consists of the personal data that is more variable but still useful to identify a user, usually consists in temporary data such as address or physical characteristics.

The external ring contains those attributes related to an identity but sector-specific, such as personal data regarding healthcare records, driver license, and tax record.

To access a digital service, there is the need for at least one of the attributes pertaining the digital identity to be unique, to allow individualization between of users. These attributes are called "identifiers". (Wayman, 2008).

Static information is the most frequently used method for identifying someone. Most financial companies or merchants use static information to verify identity. Static information was thought to provide security because that information was supposedly outside of the hands of criminals and not guessable. However, static information doesn't get updated, meaning that the longer data is there and the more likely it is to become compromised. (Gafke[20], 2017)

For security reasons, new technologies are enabling a second approach, called "dynamic verification". This form of digital identity is based on iterative processing of multiple sources of information, including social media activity, geolocation, etc. (BBVA, 2018). Continuous assessment and monitoring are crucial to support this system, and it is most used on self-asserted digital identities, where the LOA is low, to ensure a good level of security without significantly impacting on user experience.

Current trends are heading towards a mixture of both approaches, considering both static and dynamic factors in the management of digital identity (BBVA, 2018).

Today, four types of attribute groups are available to connect identify an individual: (BBVA, 2018).

- What the individual knows (password, PIN, security code).
- What the individual has (identity card, bank card).
- What the individual looks like or how he behaves (biometrics spanning physical/behavioral features).
- Where the individual is (mobile number, geo-location, IP address, social network site).

[20] Gafke, "Moving from static to Digital Identity" (2017) https://www.forbes.com/sites/forbesfinancecouncil/2017/10/10/moving-from-static-identity-to-digital-identity/?sh=62e542e7133f

## 2.8. Models

The landscape of Digital Identity systems is heterogenous and varied. The Digital Identity Observatory of Politecnico di Milano studied these systems and categorized them in 5 macro models:

- Social ID, the typical identity system associated with a social platform account. In this model basic data are acquired though self-declaration in the registration phase, leading to a low level of assurance, dynamic data are frequently updated and enriched. Facebook and Google are two examples, this identity can be used to access other low risk digital services.
- eCommerce ID, this identity system has similar characteristics to social ID, but it refers to commercial platforms and marketplaces. Amazon and Alibaba are examples.
- Mobile ID, based on the possession of a Sim card as a secure element for identity data, the identity is verified during the purchase of the Sim card, permitting a medium-high level of assurance. This model usually takes advantage of the providing company established reach, and their customer relationship management experience (European Commission, 2020[21]). Moreover, it can be more accessible to transient workers, underbanked or even and stateless individuals (Gartner[22], 2019). The main example is GSMA Mobile Connect, a standardized and globally interoperable infrastructure, many major telecommunication providers adhered to this solution (e.g., Vodafone, Orange, Telia).
- eGov ID, this model gathers the digital identity systems developed and distributed by government entities. These systems are generally characterized by a high LOA and are mostly used to access public services, e.g., electronic identity cards.

[21] European Commission, "Business trends report – Bring Your Own Identity" (2020)
[22] Gartner, "Innovation Insight for Bring Your Own Identity" (2019)

- Financial ID, the profile of data gathered by financial institution (i.e., banks); this model has a high Level of Assurance and has been used to access external services, as in the case of the Swedish digital identity system BankID.

These models can be divided in two macro categories: on one side there are Social and eCommerce ID, with a low LOA and a high use frequency; on the other side Mobile ID, eGov ID and Financial ID are identity systems with a much higher LOA and a lower use frequency.

Focusing on the trusted identity models, Financial ID and Mobile ID are business oriented, leading to a rich data set and a good user experience, while eGovernment ID usually struggles to step up into the business world.

## 2.9. Actors

Cao and Yang (2010) identified three core components for digital identity systems: user, service provider and identity provider, while the World Economic Forum (2016) defined 4 roles every identity system must have to operate:

- **Users**, individual citizens and clients are the end users of digital identity. They enroll into the identity system and are provided with credentials, allowing them to engage in transactions.

- **Identity Providers (IdPs)**, which are the entities holding the attributes, attesting their veracity, creating digital identities for the users by registering them, and completing the transactions on behalf of the users.

  A key issue for IdPs is the validity that others give to the veracity of the attributes of their digital identity (BBVA, 2018; World Bank Group, 2016).

  BBVA digital identity research (BBVA, 2018) identified two macro categories for IdPs: public and private.

- **Public sector IdPs**

  Governments have always been identity providers for physical identity documents, as passports or identity cards. Many governments are acting nowadays as IdPs for digital identity systems, and these national eIDs are usually issued in order to provide access to government services.

- **Private sector IdPs**

  Private companies have the necessity to identify customers attributes to create a corporate identity. The private IdPs transform individuals into users through the creation of credentials.

- **Service Providers (SPs)**, also known as Relying Partners (RP) (Gartner, 2019), which are the entities accepting the identity from the IdP and allow users to access their services.

  This may include public agencies as well as private service providers. Different services require different level of assurance, hence the choice and relation with a trusted IdP is fundamental (World Bank Group, 2016)

- **Governance Body**, regulatory agencies or institutions who oversights the system legal standards and requirements for the collection, storage, and use of personal data.

The World Bank Group[23] gives a broader categorization of the different roles, taking into account the technological requirements of the system and the various partners who can support IdPs and SPs. Four more prominent roles are considered:

- Attribute providers: are entities that hold verified user data and either verify or provide these attributes to third parties, often the same actors play both the role of attribute and identity provider.

[23] World Economic Forum, "A Blueprint for Digital Identity" (2016)

- Authentication providers: it is the entity who verifies that the user has the right to access a specific service, usually Service Providers play this role.
- Information Provider, it is the entity who verifies the information of the user's identification documents, this role is not present in low LOA identity systems.
- Technology Providers: which manage and provide the technological structure to the whole system.

## 2.10. Phases

The identity lifecycle is a process that starts when a person applies for Digital identity and ends when the record is removed. According to the World Bank Group (2016), this process can be divided in 5 phases, which are Registration, Issuance, Authentication, Authorization, and Identity Management. These activities are strongly connected, in fact we can say that they form a chain of interdependence: authorization depends on authentication, which depends on issuance and registration (Jovanovic et al., 2016).

### 2.10.1. Registration

"Registration is the most important step in digital identity" (World Bank Group, 2016). According to the World Bank Group[24], registration involves users and IdPs, and can be divided in Enrolment and Validation.

**Enrolment** is the first step of authentication, key identity attributes are acquired from a person who claims a certain identity, which may include biographical data and biometrics. The set of attributes asked to the user have important implications

[24] World Bank Group, "Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation" (2016)

on utility, interoperability and on the level of assurance of the system. "In-person proofing is required for the highest identity assurance level" (World Bank Group, 2016).

**Validation** occurs after enrolment, the identity a user has claimed is validated by checking the attributes presented against existing data. The authority determines the authenticity, validity, and accuracy of the identity information the applicant has provided and relates it to a living person. During validation of high LOA systems, it is established if the identity satisfies the three following properties:

- Existence/Liveness: the person exists at the time of enrolment and can be localised, meaning that some attributes are acquired thought the which that person can be reached (address, phone number, email).
- Uniqueness: it is verified that one individual claims one identity, this process is also called de-duplication, and can be accomplished using combinations of a variety of attributes.
- Linkages: the registering identity can be linked to other social identities, such as those in civil registries, population registries, tax registries, etc.

### 2.10.2. Issuance

Issuance is when credential management comes into play, it is the process of creating and distributing virtual or physical credentials. Traditionally identity issuers provide documents or credentials. For an identity to be considered digital credentials must be stored and communicate data electronically. Types of electronic credentials include (World Bank Group, 2016[25]):

- Smartcards, usually characterized by advanced security features, are able to record and communicate user's credentials and data through an electronic

[25] World Bank Group, "Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation" (2016)

chip. Near Field Communication technology (NFC) is commonly used for these purposes, as in the case of the Italian CIE (Carta di Identità Elettronica).

- 2D bar code cards: smartcards can be personalized with an encrypted 2D bar code, either in combination or substitution of a chip.
- Mobile Identity: Mobile phones and other devices can be used to provide portable digital identity and authentication for several online transactions, for example using SIM cards.
- ID in the cloud: systems whose credential, certificates and biometrics are stored and exchanged on servers only. Cryptography and a tamper resistant environment will increase the security of the system.

### 2.10.3. Authentication

Authentication is the process of verifying an identity claim, operated by a user though a computing device (e.g., mobile phone), against the information registered on an online service. (World Bank Group, 2016; Shah and Kanhere, 2019)

Authentication is needed for the user to access the desired services. The user, depending on the system, uses one of the electronic credential pathways discussed before, being smartcards, mobile identity, and ID in the cloud, to provide personal or possessed information that the system confronts with the registered attributes and requirements.

Security in the authentication process is fundamental since an unauthorized access could expose important private data and have serious repercussions like loss of money (Shah and Kanhere, 2019). Thus, authentication is about establishing the validity of a proof of identity.

A proof of identity can be any piece of information that an authentication server accepts, this information can be a personal identification number, a password, biometric data, or a combination of these, according with the factors discussed in the “attributes” chapter: what an individual is, owns, knows or does.

Depending on what type of and how many attributes are needed to authenticate, three different authentication types can be distinguished, with an increasing level of security:

1. Single-factor authentication: that is mostly represented and widely used as the user-password model.
2. Two-factors authentication: TFA couples the representative data (username/password combination) with the factor of personal ownership, such as a smartcard or a phone.
3. Multi-factors authentication: it is a secure process of authentication which requires more than one authentication technique chosen from independent categories of credentials. It provides a higher level of safety and facilitates continuous protection of critical services from unauthorized access. From the most part MFA is based on biometrics, which is automated recognition of individuals based on their behavioral and biological characteristics (Ometov and Bezzateev, 2018; Dasgupta et al., 2017).

In Figure 2.2, a summary of authentication types and their enabling technologies.


Figure 2.2 - Authentication types

The real challenge for authentication is to manage the tradeoff between an adequate LOA and the security measures on user experience.

### 2.10.4. Authorization

Authorization is the decision to allow a particular action based on an identifier or attribute. It takes place after an individual claim for identity is authenticated, it is the process by which the SP defines and grants the access rights to the user. The SP determines the requirements for transaction eligibility and make a query about certain user attributes (World Economic Forum, 2016).

Specifically, "authorization is an approval given to the user, application program or a process to accesses a particular object or group of objects" (World Bank Group, 2016).

This is the first and only phase that does not depend on the Identity provider, being user and service provider the main involved roles (World Bank Group, 2016).

Within the company context, the authentication is generally managed through tools of Identity and Access Management or Privileged Access Management (Witty et al., 2005).

### 2.10.5. Identity Management

Identity Management (IdM) is not a proper phase, it is instead the continuous process of retrieving, updating, and deleting identity data attributes, data fields and policies regarding users' access to information and services. IdPs manage identity data through a dynamic process, this includes updating, reproofing, and revoking identity attributes over time, including personal data and credentials.

The International Communication Union (2009[26]) identified a comprehensive definition: IdM is a set of functions and capabilities used for:

- Assurance of identity information (e.g., identifiers, credentials, attributes)
- Assurance of the identity of an entity (e.g., users, groups, user devices)
- Enabling business and security applications.

[26] International Communication Union, "NGN identity management framework" (2009)

According to Cao and Yang (2010) IdM is an integrated system of business processes, policies and technologies that enables organization to facilitate and control user access to online application and resources.

Challenges of IdM include to maintain a cost-effective system, to improve system performances by using data analysis, ensure databases are updated, to maintain privacy and security controls, and to protect personal and business information from unauthorized users. (World Bank Group, 2016; Cao and Yang, 2010).

## 2.11. Archetypes

Cao and Yang (2010) described three models for identity configurations: isolated, centralized, and federated. Each model is characterized by different characteristics, number and allocation of tasks for Users, IdPs and SPs, as shown in Table 2.1.

| Model | SP Type | IdP Type | Service Composition | Cross Domain Access | Identity Storage | User Control over Identity | Privacy Protection |
|---|---|---|---|---|---|---|---|
| Isolated | Single SP and IdP, SP is IdP | Single IdP and SP, IdP is SP | Sole Service | No support | On SP | No control | Few and very weak protection |
| Centralized | Multi SPs | Single IdP | Multi services but in the same domain | Limited support | On IdP | Few control | Much but weak protection |
| Federated | Multi SPs | Multi IdP | Multi services from multi domains | Nearly full support | On both SPs and IdPs | Much control | Much and strong protection |

Table 2.1- Models for identity configurations (Cao and Yang, 2010)

According to them, IdM paradigms can be classified into network-centric paradigm, service-centric paradigm, and user-centric paradigm:

- The network centric paradigm occurs when the IdM system is established and operated by a single entity for a fixed user and resource community
- The service-centric paradigm, instead, is composed by services of multiple SPs that operate across multiple domains.
- The User-centric paradigm is the most modern form of IdM, users become the focus of the IdM, the control of identity shifts from SPs to users. Users can decide what attributes to share and under what circumstances.

More recently a different categorization took over, in which isolated and centralised models are merged, and the decentralised model was added. Accordingly, identity ecosystems are classified into three archetypes: centralized, federated and decentralised (World Economic Forum, 2018; Dib and Toumi, 2020).

According to Pohn and Hommel (2020), decentralised archetype is furtherly divided into 2 archetypes, being user-centric and Self-Sovereign Identity (SSI). BBVA (2018) and Sovrin (2017[27]) agree with this latter categorization, and affirm that identity management system is evolving, dividing its state in four phases, with SSI being the final step (Figure 2.4):

Centralised Identity, Federated Identity, User-Centric Identity, Self-Sovereign Identity.

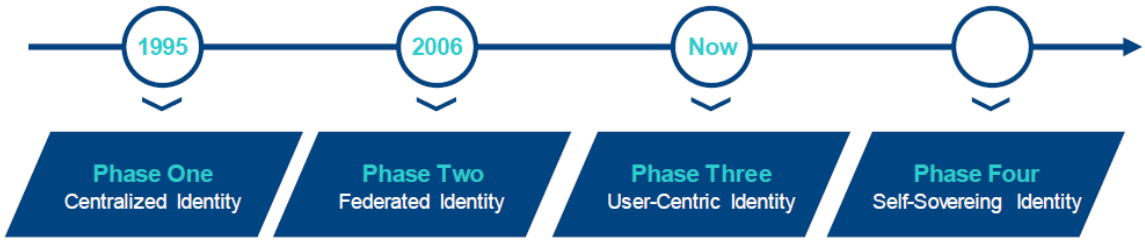



Figure 2.3 – Modern archetypes (Allen, 2016)

[27] Sovrin Foundation, "The Inevitable Raise of Self-Sovereign Identity" (2017)

The following paragraphs have been written according to the latter classification.

### 2.11.1. Centralized Identity

In the centralized identity the system has single central authority, where users' data and credential are stored (European Commission, 2020); this single IdP is the owner or manager of the system (World Economic Forum, 2018), and authenticates users and supports individuals' transactions with SPs.

This model has been widely adopted by governments in their national digital identity systems, in some cases because the law mandates its use. This system potentially provides a high LOA since the owner of the system determines the level of due diligence based on regulation. On the other hand, centralisation gives owner power that, if unchecked, leaves the door open for incorrect behaviour (World Economic Forum, 2018).

### 2.11.2. Federated identity

A federated system is formed when two or more centralised systems establish mutual trust by mutually recognizing each other's trust and proofing standards (World Economic Forum, 2018).

In the federated model, protocols including policies and technology standards are shared between SPs, so that identities from different identity domains can be recognized over all domains (De Angelis et al., 2016), therefore solving the problem of portability and meaning that individual service providers' platforms do not need to build their own identity management infrastructure (European Commission, 2020).

The World Economic Forum in 2016 also defines the archetype of **Federated Authentication**: In the federated authentication system, a primary IdP uses a set of third parties secondary IdP to authenticate users to a range of SPs. These systems are designed to enable the primary IdP attributes to be used across multiple service

providers, delegating processes to secondary IdPs. This is the case of the Italian system SPID.

In the Federated model, complexity arises for the system owners from the potential need for legal agreements, including the division of risks and liabilities, and for shared data and technical standards (World Economic Forum, 2018).

### 2.11.3. User-Centric identity

The User-Centric Identity is an evolution of the federated configuration, where the user gains more control over the use of its identity in a widely interoperable ecosystem. Cameron et al. (2008) stated that "the core requirement for user control is that the flow of information from Claims Providers (IdPs) to Relying Parties (SPs) only happens at the request of the user."

In these systems many IdPs collect, store and transfer user attributes to many SPs. These systems do not rely on attributes emitted by a single IdP and enable users to make use of information managed by many entities.

User-centric identity systems are developed to give users more control by allowing them to choose IdPs independently from SPs. The goal of a user-centric identity system is to enable the creation of IdPs that operate in the user's interest rather than in the sole interest of the SP.

In the User-centric identity system usually user's authentication is centralized, password based, and wholly dependent on IdPs (Anderson-Priddy and Toth, 2019), not solving the problem of security, since centralised system administration could easily be target of cyber-attacks (BBVA, 2018).

### 2.11.4. Self-Sovereign Identity

SSI is the next step beyond user-centric identity, where the user is central to the administration of identity; that requires not just the interoperability of a user's

identity across multiple locations, but also true user control of the digital identity, creating user autonomy (Allen, 2016).

SSI is independent from any individual silo, and provides control, security, and full portability. It removes centralised external control. The individual to whom the identity pertains completely owns, controls, and manages their identity. In this sense the individual is their own IdP, since there is no external party who can claim to "provide" the identity for them because it is intrinsically theirs (Sovrin, 2017).

In the SSI configuration the user is the owner of its identity, fully in control of its attributes and their exchange; people and businesses can store their own identity data on their own devices and provide their identity to those who need to validate it, without relying on a central repository of identity data.

Accordingly, in a SSI system users exist independently from services, users are able to control their digital identities and when central authorities have no authority over them (W3C, 2018; Allen 2016).

Anderson-Priddy and Toth, in 2019, merged the works of Allen (2016), The World Wide Web Consortium (2018) and Cameron (2005), and identified the properties of Self-Sovereign Identity:

- **Identity data model, persistence, and portability**

  A common identity data model is needed to support the specification of digital identities comprising self-sovereign claims.

- **Consent and disclosure**

  Users should be able to give consent and disclose just enough private information to satisfy the needs of relying parties.

- **Interoperability**

  Owners and providers must be able to use their digital identities to interact with each other reliably and securely over the web.

- **Secure Identity transfer**

  Owners should be able to securely transfer their digital identities to other parties, especially when specifying sensitive data.

- **Usability**

  User's interfaces are key to the success of a digital identity system, usability means that the owner can effectively control their data.

- **Counterfeit prevention**

  Data and attributes need to be reliable.

- **Identity verification**

  Owners of digital identity must be able to prove who they are.

- **Identity assurance**

  Along with Counterfeit prevention, a high Level of Assurance is key to the system to operate.

- **Secure transactions**

  Once their digital identities have been securely transferred, owners should be able to use their digital identities to secure their transactions and maintain their privacy.

Self-sovereign identity is the concept of an identity and related data that are controlled and owned by the individual or consumer (Gartner, 2019). The application of SSI in a digital identity solution is made possible by the Blockchain technology (Hong and Kim, 2020).

## 2.12. Blockchain

A blockchain is one type of a distributed ledger that consist of replicated, shared, and synchronized data over the internet, it was introduced as the backbone of the Bitcoin cryptocurrency, and rapidly grew in popularity. Blockchain is able to record transactions using cryptographic tools, these cryptography functions of blockchain technology enable integrity of ledgers, authenticity of transactions, and privacy of transactions without the necessity of a centralized data storage for maintaining its data (Li et al, 2017; Lee, 2017).

It is important for IdM because an integration of this technology would be able to solve some prevalent questions, such as centralized governing of identities, which has some security and availability issues. Moreover, blockchain eliminates the need for trusted third parties to perform checks on identities, as the blockchain ledger is distributed across the consortium participants (Bouras et al, 2021).

Technically is composed by a chain of blocks of valid transactions in a peer-to-peer network, each block includes the hash to the prior block in the blockchain. Thanks to this structure, all the participants nodes of the blockchain have access to the information registered at any time, and if a node is being attacked, the other members of the blockchain could isolate and avoid the "fake block" (Lim et al, 2018; Páez et al, 2020).

Distributed Ledger Technologies could positively impact Identity Management according to the following characteristics: (Dunphy and Petitcolas, 2018; Lim et al., 2018)

- **Decentralized** – Identity information is not controlled by any single centralized authority.
- **Tamper resistant** – Historical activities in the DLT cannot be tampered with, and transparency is given to all changes to that data.
- **Inclusive –** Blockchain expand the reach of legal identities and reduce exclusion.

- **Cost effective** – Shared identity information can lead to cost savings for the involved actors along with the potential to reduce the volume of personal information that is replicated in databases.
- **User control** – Users cannot lose control of their digital identifiers if they lose access to the services of a specific identity provider.
- **Fast –** Transactions are much faster than in a centrally controlled system.
- **Disintermediated –** DLT has a peer-to-peer nature that does not require third parties.
- **Immutable –** Transactions in the blockchain cannot be altered.
- **Permanent** – A public blockchain will act as a public ledger, data will be accessible if the blockchain remains active.

## 2.13. Digital wallet

A digital wallet is a virtual storage system that can capture one's identity and digital credentials that provide a person to commit an electronic transaction. (Hassan and Shukur, 2020) It usually takes the form of an application for electronic devices as smartphone and computers. In a digital wallet users can register themselves, insert their data and make transactions. The main use of wallets refers financial services, such as payments, with the aim of providing a digital form of a physical wallet, and later extended to uses outside of the financial field, mainly involving certified attributes (Fainusa et al., 2019).

The Digital Wallet saves all the identity related personal and confidential data which is owned by the user, and the user exercises control over its data by the use of a digital device, typically a smartphone.

Digital wallets are the model through which the SSI paradigm is implemented as a digital identity solution.

In a SSI digital wallet, third parties IdPs are removed since not needed, it is a peer-to-peer model and users and organizations are offered direct connectivity (Naik and Jenkins, 2020).

Thanks to distributed ledger technologies, users are allowed to encrypt their personal information into private keys and store them in identity wallets that can be installed on mobile devices or PCs.

These private keys remain under the users' exclusive control, who in turn can decide whether to grant third parties access to them or not. This model grants users complete control over their personal information, so that they can decide what information to include when sharing identity data, and with whom to share it. This model requires a verifying actor, represented by a trustworthy institution, such as governments, insurers, banks, mobile network operators, or any organization which belongs to the decentralized identity providers' network.

The Business Trends Report of the European Commission (European Commission[28], 2020) individuated advantages and challenges for this model.

Advantages are:

- In digital wallets, users are in the position to decide what use is made of their identity data, protecting themselves from the risk of identity theft.
- Thanks to the blockchain technology, the trusted party issuing the digital certificate will not know that a proof or an attestation was requested by the user, impeding user tracking.
- Security, since the decentralization of data storage significantly limits the risk of hackers gaining unauthorized data access to thousands or million identities in one attack.

Challenges are:

- The achievement of digital wallets benefits is strictly correlated on how populated the ecosystem is, both in terms of users and SPs.

[28] European Commission, "Business trends report – Bring Your Own Identity" (2020)

- The absence of third parties IdPs creates problems when a user loses its private key.
- The enhanced privacy granted to the user can have a backfiring effect with non "honest" actors. Users might be tempted to disclose only the information strictly requested by the SP, hiding information that could negatively impact their reputation.

## 2.14. European digital identity wallet

In June 2021 the European Commission proposed a review to the regulation eIDAS[29] (Electronic Identification, Authentication and Trust Services), announcing a framework for digital identity that will be available to all EU citizens, residents, and businesses in EU. The European digital wallet is meant to operate through the aggregation of national identity systems of EU member states. In fact, the majority of European countries are developing or have already developed national identity systems, and the European Commission invited all the member states to establish a common toolbox by September 2022, in order to favour standardization and integration between the solutions.

The proposed European digital wallet will allow citizens to prove their identity and share electronic documents from their European Digital Identity wallets with the click of a button on their phone. They will be able to access online services with their national digital identification, which will be recognized throughout Europe.

The European Commission stated that the new European Identity will be:

- **Available to anyone who wants to use it**, if being EU citizens, residents or businesses.
- **Widely usable**, for the purpose of accessing public and private services.

[29] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

- **Users in control of their data,** with users that will be able which part of their identity attribute to share with service providers.

## 2.15. Biometrics

Biometrics for digital identity purposes is strictly related to user identification and authentication. O'Gorman, in 2003, defined biometrics as "a feature measured from the human body that is distinguishing enough to be used for user authentication", including a wide variety of known and unknown traits, such as: fingerprints, eye, face, hand, voice and signature. Biometric authentication establishes a person's identity based on something she is, rather than something she possesses or remembers.

Accordingly, biometric recognition, or simply biometrics, refers to recognizing a person based on one or more of his anatomical or behavioural characteristics (Prabhakar et al., 2011).

Biometrics proved to have a strong appeal in digital identity management, given that they can connect bodily people to identity records to create a one-to-one correspondence between people and records and provides greater security and convenience than traditional methods of personal recognition (Wayman, 2008).

Biometrics, as an attribute, are labelled as describing "who you are" which is very hard to mimic, fingerprints, iris, face etc. are unique personal features, exploitable to determine a person's identity, something that passwords and tokens cannot do, since they can be lent or stolen. (Bromby, 2010; O'Gorman, 2003).

A biometric system can operate either in the authentication phase, where a claim of identity is submitted together with the captured biometric data, or in the identification phase, where the attributes of an individual are collected.

Prabhakar et al. in 2011 identified the characteristics of good biometric traits: they should be measurable, distinctive (unique for every person), stable over time, non-intrusive and easy to use.

Biometrics may serve a variety of function, that can be summarized in five categories (Prabhakar et al., 2011):

1. Secure access to something or somewhere
2. Secure data storage
3. The verification of consent for particular actions
4. The verification of identity for particular persons
5. The non-repudiation of information

Biometrics can be either be used combined with other types of authenticators, such as passwords or tokens, resulting in a multi-factor authentication, or it can be used, as in most cases, to substitute other authentication method for the sake of convenience, permitting users to avoid remembering or digiting a password.

## 2.16. Literature Gap and Research Questions definition

Digital identity has high relevance for individuals, organizations, governments, and objects, as identification represents a necessary basis for transactions. Since transactions increasingly take place directly between objects and devices, without human intermediation, secure methods of digital identification become even more important (Ante et al., 2022).

The growing importance of digital identity interested scholars and academics, resulting in a broad extension of literature streams. Design and characteristics of digital identity solutions and ecosystems were analyzed, studying performances and evolution in the business field.

Further research investigated the macro-economic, political, and social benefits of digital identity, unveiling its potential as a tool for inclusive development, and therefore encouraging governments to promote national solutions.

Down this line, guidelines and best practices for ecosystem configurations, actors and their interactions have been formulated, with the aim of providing citizens with a unique digital identity, to be used for their digital interactions within the public and private world.

Benefits of a diffused digital identity solution for the society have been in-dept discussed and analyzed, as well as common principles for fully unlocking its value. Even if digital identity and its evolution are a central topic of the modern digital scenario, some fronts of research remain open.

The academic context lacks a comprehensive framework for guidelines and a roadmap on how to achieve a critical mass, both of users and SPs, able to trigger a chain reaction for mass adoption.

Specifically, while governments can support national solution to some extent, especially regarding public service providers and diffusion among users, it is not clear what elements may constitute a sufficient advantage for private service providers, in such a way to originate a natural willingness to join the ecosystem.

National digital identity systems serve as their primary purpose to permit interactions between citizens and public services. These services often feature a high level of criticality, and therefore require a high LOA to be accessed. Thus, national digital identity systems are characterized by a high LOA.

For these reasons, industries where a high LOA recognition of their customers are most likely to be interested in the adoption of these systems. By this logic, banking, insurance, and utility industries have been individuated as focus of this research.

The definition of the research question must be taken considering the research gap this thesis aims to bridge. Moreover, a certain degree of openness and broadness is recommended to allow flexibility (Eisenhardt's, 2007).

The research questions are so formalized:

- In what way companies of banking, insurance and utility industries are managing the digital identity of their customers?
- What drivers and barriers affect the evaluation of national digital identity systems in these industries?

# 3 METHODOLOGY

In this chapter both the methodology and the selected case study will be described. The objective of this research is to understand drivers and barriers for the adoption of a national digital identity system by the private sector.

A practical and empiric approach has been taken, to retain the "the holistic and meaningful characteristics of real-life events" (Yin, 2003), to formulate a relevant, solid, and testable theory (Glaser and Straus, 1967; Eisenhardt, 1989a; Feldman and Orlikowski, 2011).

In order to grasp the many facets of the dynamics involved in companies decision-making process, a qualitative rather than a quantitative analysis has been developed, adopting an interpretative and inductive perspective (Eisenhardt, 1989b) based on case studies (Eisenhardt, 1989a).

Firms belonging to the financial, assurance and utility industries have been involved in the research, since these sectors have been identified as those that would benefit the most by the adoption of an external, and certified, digital identity system.

## 3.1. SPID and CIE as units of analysis

The choice of the unit of analysis is fundamental in conducting case-based research. In this process, the contextual conditions of the case play an important role, since the boundaries of the case and the context are not always easily identified (Yin,

2003). Moreover, since the purpose of this research is not to test a theory, but to formulate one, theorical sampling is appropriate (Eisenhardt, 1989; Yin, 2003).

Considering the context, and the Italian scenario, the cases of SPID and CIE have been selected as the most suitable to purse the research objective.

SPID or Sistema Pubblico di Identità Digitale, is the most widespread national digital identity system in Italy. It was initially conceived in 2014 by the National Agency for Digitalisation (Agenzia per l'Italia Digitale, in Italian; hereafter AgID), a public agency established by the Italian government in 2012 responsible for the digital transformation of the Public Administration in Italy.

CIE or Carta d'Identità Elettronica (Electronic Identity Card), is the national card-based digital identity system in Italy. It is the smart equivalent of the traditional identity card and acts both as a physical document and a digital identity solution; it was first released in 2016 and it is provided with a chip capable of exchanging information through NFC technology.

Since 2016, SPID and CIE have been supported by the "Team per la Trasformazione Digitale", a technical agency under the Italian ministry of technological innovation. Team per la Trasformazione Digitale is composed by experts and has the aim of exercising powers of impulse and coordination, as well as providing information to public and private entities for the implementation of essential actions, initiatives and works, connected and instrumental to the implementation of the Italian Digital Agenda, also in line with the objectives of the European Digital Agenda.

The objective of these projects is to provide Italian citizens with secure identity systems, allowing them to digitally access public and private services with a unique set of trusted credentials. Moreover, both these systems have been recognized as compliant to eIDAS, and soon it will be possible to access through these means many public institution portals across Europe.

### 3.1.1. SPID

SPID is a "Bring Your Own Device" (BYOD) Digital Identity. Basically, SPID users authenticate by accessing their Identity Provider's app on their own device (usually a smartphone), since the system does not rely in any physical tool issued by the IdP, as in the case of Sim or ID cards.

The configuration of the ecosystem is Federated Authentication, described by the World Economic Forum in 2016 and shown in Figure 3.1; meaning that many private companies have been involved by AgID as project partners, this type of architecture enables a profitable economic structure for SPID, allowing a national identity system without requiring the use of public investment.

AgID oversees the regulatory and strategic development of the platform, in partnership with nine Identity Providers, which are public and private organizations, and are in charge for the registration and the issuance of SPID.

SPID structure is shown in Figure 3.1.

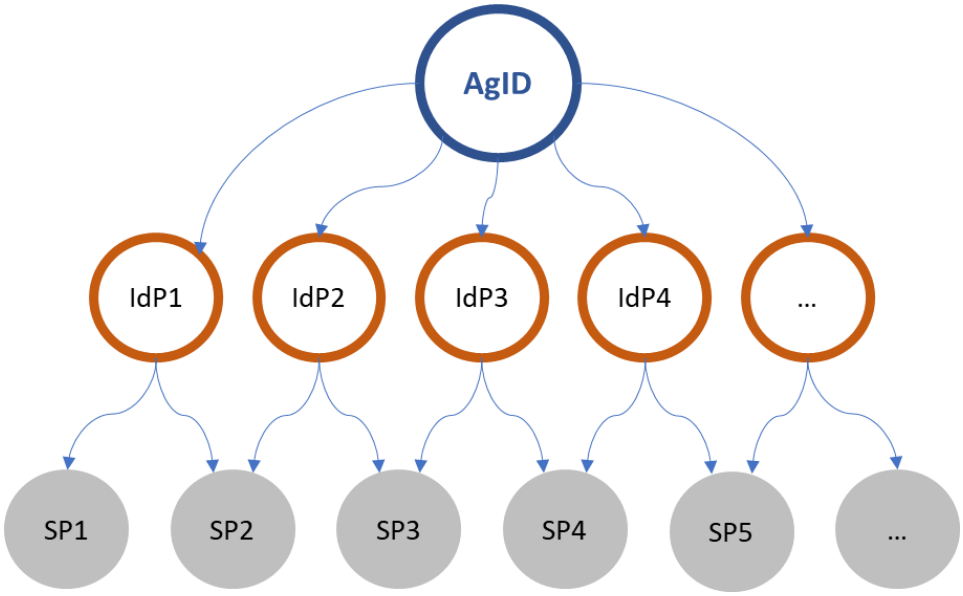



Figure 3.1 - SPID architecture

These actors consider SPID as a project of digitalization of the country and as a business opportunity, once a consistent number of citizens and SPs have been pulled abroad.

The economic sustainability of the project relies on private SPs: SPID issuing to citizens is totally free, and Service Providers willing to authenticate their users through SPID will be recognizing a fee to IdPs in exchange for the service.

Three levels of SPID are available. Each level corresponds to a different LOA:

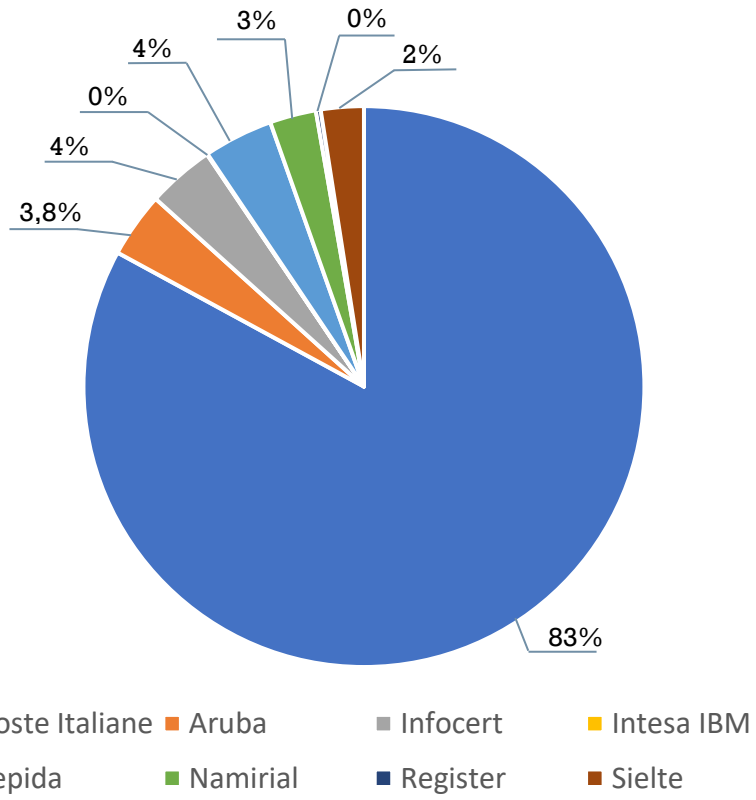
- Level 1 SPID: allows the access to online services through the use of a user and a password
- Level 2 SPID: allows the access to online services through the use of a user and a password, plus the generation of a One Time Password (OTP), to be provided via app or SMS.
- Level 3 SPID: allows the access to online services through the use of a user and a password, plus a specific physical support holding cryptographic keys. This support can be a smart card or a remote digital signature device.

To a higher level of SPID corresponds a larger fee to be paid by the SP to the IdP.

Three companies were involved together with AgID as IdP since the beginning, being TIM Trust Technologies, Poste Italiane and Infocert, as they were already partners of AgID for other qualified services, such as certified signature and certified email.

Subsequently, after some months, other six companies, for a total of nine, have joined the network of IdPs, which are Aruba, Sielte, Register, Namirial, In.Te.S.A. and Lepida.

As shown in Figure 3.2, Poste Italiane issued the vast majority of SPID identities, data gathered by the Digital Identity Observatory of Politecnico di Milano[30] (2022).



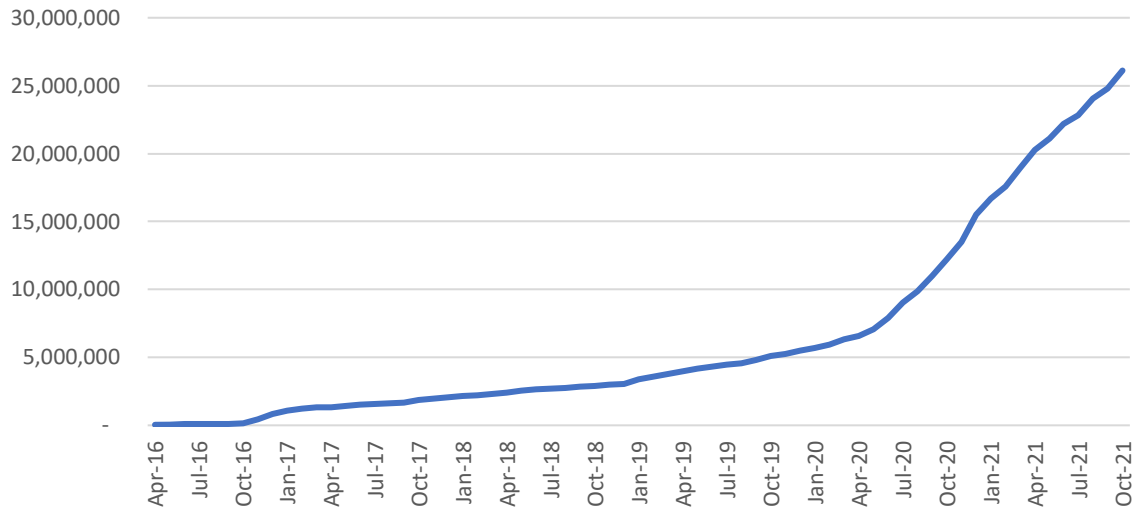

Data gathered by the Digital Identity Observatory of Politecnico di Milano

Figure 3.2 – Releases of SPID among IdPs

Concerning SPID diffusion, it was firstly released in 2016, having a steady and slow growth and reaching roughly 5.4 million releases at the start of 2020. Initially SPID was supported by the government with spot initiatives, in the form of bonuses that could be claimed with SPID only, that created a moderate diffusion but scarce

[30] Digital Identity Observatory of Politecnico di Milano, (2022), *SPID: DIFFUSIONE E UTILIZZO DEL SISTEMA PUBBLICO DI IDENTITÀ DIGITALE* https://www.osservatori.net/it/prodotti/formato/report/spid-diffusione-utilizzo-sistema-pubblico-identita-digitale-report

utilization. In fact, most of the time, users registered to SPID to benefit from an occasional service, and rarely continued using the solution for other purposes. The turning point happened with 2020 and the global pandemic, SPID had an explosion in diffusion thorough both 2020 and 2021, reaching 26.1 million users in the month of October 2021 (Figure 3.3) and 60,000 monthly authentications.




Data gathered by the Digital Identity Observatory of Politecnico di Milano[31]

Figure 3.3 – Growth of released SPID

Another relevant metric to understand SPID usage and coverage is the number of SPs; at the time of writing this thesis, 9,519 public administrations allow access to their web services through SPID, both at local and national level, while there are only 88 private SPs registered in the SPID ecosystem.

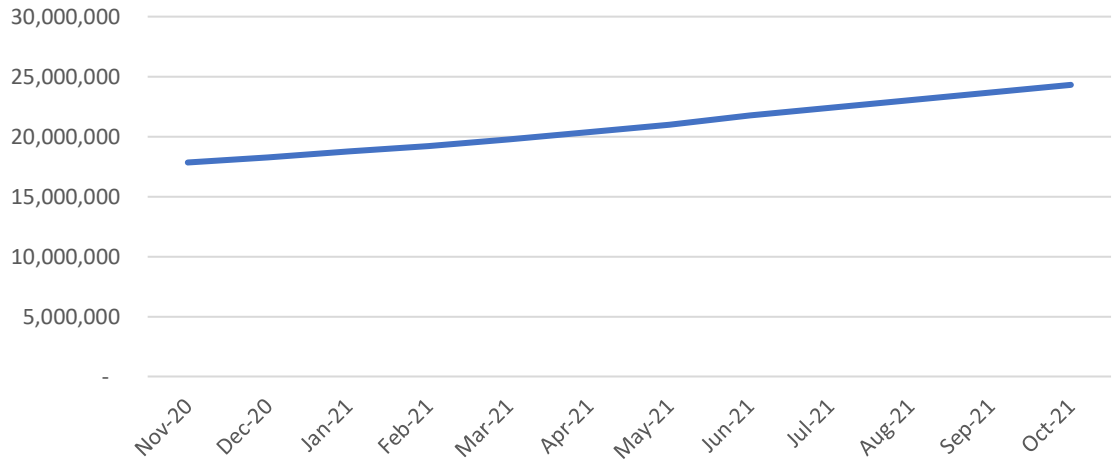
[31] Digital Identity Observatory of Politecnico di Milano, (2022), *L'EVOLUZIONE DI SPID E CIE NEL 2021* https://www.osservatori.net/it/prodotti/formato/video/evoluzione-spid-cie-2021-video

### 3.1.2. CIE

CIE or Carta di Identità Elettronica, is the national identity system in Italy based on smart card. In addition to being a valid physical identity document, CIE digital capabilities are accessed through the reading of a chip implemented within the card: this process can happen with a contactless chip reader, or by using NFC technology on any smart device (e.g., smartphone), and authenticating through to a dedicated app.

CIE architecture is centralised, it is issued by the Ministry of the Interior, and the app is released by the Italian Bureau of Engraving and Printing (Istituto Poligrafico Zecca dello Stato).

Considering the diffusion, the modern version of the document, CIE 3.0, has been initially released in 2016; in October 2021 24.7 million of citizens are in possess of it (Figure 3.4). However, the double role of digital and physical document results in many people using it for the latter purpose, and not exploiting its digital capabilities. Accesses cannot be easily quantified since public data are not available.




Data gathered by the Digital Identity Observatory of Politecnico di Milano[32]

Figure 3.4 – Growth of released CIE

[32] Digital Identity Observatory of Politecnico di Milano, (2022), *L'EVOLUZIONE DI SPID E CIE NEL 2021* https://www.osservatori.net/it/prodotti/formato/video/evoluzione-spid-cie-2021-video

Regarding Service Providers, in October 2021 there are 1,790 public administrations accessible through CIE, while the number of private SPs stops at 3.

## 3.2. Additional considerations

The adoption of these identity systems has been strongly incentivized by the Italian government, firstly by promoting one shot-initiatives, such as bonus accessible only through a national digital identity system. Subsequently by regulation acts: since October 2021 SPID and CIE are the only means through which citizens can access online public services, ranging from municipality websites to institutional services. These initiatives accomplished great results in promoting the diffusion of both the solutions, that experienced a rapid increase in growth since the start of 2020. On the other side, this created a large discrepancy between the numbers of public and private SPs for both SPID and CIE.

Moreover, regarding CIE, the interactions that happen through contactless reader cannot be tracked, resulting in no available data in matter of uses. A survey[33] conducted by the Digital Identity Observatory of Politecnico di Milano found that only one third of CIE owners used its digital capabilities at least once.

[33] Digital Identity Observatory of Politecnico di Milano, (2022), *SPID: DIFFUSIONE E UTILIZZO DEL SISTEMA PUBBLICO DI IDENTITÀ DIGITALE*
https://www.osservatori.net/it/prodotti/formato/report/spid-diffusione-utilizzo-sistema-pubblico-identita-digitale-report

## 3.3. Data collection

This research relied on several data sources, such as interviews, follow-up emails and archival data press releases, websites, and news articles. Moreover, it was supported by the know-how, the relationships, and resources of the Digital Identity Observatory of Politecnico di Milano, which conducted numerous studies on both the Italian and International scenario of digital identity in the last years.

In the early stage of the project, wide research on secondary sources have been conducted, consulting both regulation and latest new about SPID and CIE in order to obtain a precise idea of the ecosystem, its boundaries and critical components.

Then, a total of 15 interviews have been performed between October 2021 and January 2022 to managers of 15 different companies, comprehending 6 banking institutions, 5 assurance companies and 4 organizations operating in the utility field, as the described in Table 3.1.

| Industry | Organization | Role |
|---|---|---|
| Banking | Bank 1 | Digital Omnichannel Experience Manager |
| | Bank 2 | Innovation Manager |
| | Bank 3 | Chief Information Security Officer |
| | Bank 4 | Digital Innovation Manager |
| | Bank 5 | Chief Innovation Officer |
| | Bank 6 | Senior Digital Process Manager |
| Insurance | Insurance 1 | Digital Innovation and Transformation Manager |
| | Insurance 2 | Director of IT Business Factory |
| | Insurance 3 | Self-Care Governance Manager |
| | Insurance 4 | Marketing Advertising & Analytics Manager |
| | Insurance 5 | IT & Processes Director |
| Utility | Utility 1 | Customer Operation & Innovation Director |
| | Utility 2 | Chief Information Security Officer |
| | Utility 3 | Chief Executive Officer |
| | Utility 4 | Chief Innovation Officer |

Table 3.1 - Interviewed managers role

Each of those interviews lasted an average of 45 minutes: at the start, the scope and purpose of the research were presented, then the informant was given space to answer freely to a line-up of semi-structured questions. These questions were differentiated according to the industry of pertinence.

Subsequently the interviews have been transcribed verbatim on documents of an average of 8 pages (4.500 words).

These interviews have been designed on a common protocol that evolved systematically during the research (Eisenhardt, 1989), adapting to insights revealed in the first interviews and enabling a more comprehensive structure of questions in the latter phase of the interviewing process.

The interviews aimed to understand the dynamics behind the onboarding and authentication phases of the actors; in particular, the as-is situation of their organization, as well as drivers and barriers that could affect their willingness to adopt an external digital identity system. Subsequently, the interview turned more specifically into CIE and SPID, investigating expected benefits, barriers, and downsides of adoption.

Regarding the interviews, measures have been taken to address and minimize biases:

- **anonymity** has been promised to interviewees to encourage candour (Eisenhardt, 1989a; 1989b).
- **open ended questioning** has been used to permit informant to express their thoughts without boundaries (Koriat and Goldsmith, 2000).
- **heterogeneity** has been considered in the selection of interviewees, actors with multiple levels of hierarchy and perspective have been interviewed.
- **event tracking and non-directive questioning** (Martin and Eisenhardt, 2010) have been used as interview techniques, to yield and keep track of information during the interview itself.

## 3.4. Data analysis

Data analysis has been conducted following the Gioia Methodology, a holistic approach to inductive concept development (Gioia et al., 2012), that consists of a coding procedure of examining transcribed data, capturing and categorizing notions that describe or explain a phenomenon into variables identified as "concepts".

During the first order analysis, concepts are divided faithfully respecting informants' terms, thus leading of a large number of categories, proportional to the number of interviews and their length. Subsequently, these categories are combined, seeking for similarities and differences between them, and assigned a label, proceeding to a reduced and manageable number of categories.

The set of labels that comes out of this work goes through a second order analysis, there is a further effort of classification where concepts are categorised according to their sphere of pertinence. In this process, a triangulation between the empirical evidence of the interviews and the theoretical realm of digital identity is conducted, questioning whether the emerging themes were consistent both with the literature and the phenomena observed (Gioia et al., 2012).

As the interviews were progressing, the processes of transcribing data, coding and analysing were carried out in parallel, as suggested by Glaser and Strauss (1967), obtaining intermediate insights and ideas. As Eisenhardt (1989) stated, overlapping data analysis allowed a flexible data collection and enabled the possibility of making adjustments as the research progressed; in particular, this research took advantage from the addition of questions to the initial interview protocol.

It is important to underline that the cross-sector nature of this research implied a double dimension of analysis, firstly considering the common concepts emerged by actors of different industries, and secondly focusing on banking, insurance, and utility industries individually.

## 3.5. Enfolding literature

All along the research a continuous comparison of emergent concepts with the existing literature and previous researches has been performed. According to Eisenhardt (1989), the process of tying the emergent theories to existing literature enhances the internal validity, generalizability, and theoretical level of the case study research.

It was fundamental, during the analysis of results, to perform several checks with the supervisor of the thesis project, to ensure theoretical support and bring different perspectives on the understanding and definition of interviews' insights.

## 3.6. Evidence presentation

The chapter describing the results of the research project had to face the challenge represented by the conveying the emergent theory and the empirical evidence supporting it, while staying in the spatial constraint of the thesis.

For this reason, the result's chapter is enriched with quotes from the interviews, highlighting the emergent concepts that have twists and produce insights directly from informants' words (Gioia et al., 2012).

Moreover, the description of results in chapter 4 is structured according to both the intra-sectoral and infra-sectoral nature of the research. Firstly, industries are analysed separately; while, in the second half of the chapter, general findings resulting from a comparative analysis of the three sectors are presented.

# 4 EMPIRICAL ANALYSIS

This chapter presents the results of a research aimed to understand barriers, drivers, and opportunities for the implementation of SPID and CIE in the private sector.

SPID and CIE have experienced an exponential growth in the two-year period 2019-2020, both for voluntary factors, such as incentives and regulation disposed by the Italian Government, and for external factors, such as the necessity of using digital tools during the lockdowns caused by the global pandemic.

Although the numbers of issued credential for both the systems being very consistent, the number of private SPs stays very low and struggles to grow. This research investigates the causes of this phenomenon, focusing on three industries: banking, insurance, and utility.

These three industries have been selected as those which would benefit the most by the integration of SPID and CIE, according to their need of disposing of a secure and certified identification method to operate their businesses in critical sectors.

The main uses of SPID and CIE involve two processes:

- **onboarding**, being the process that involves the first registration of the user and the issuance of its digital identity.
- **authentication,** the process through which a user enters its credential in the SP website or app to access its services and she is recognized by the system.

Moreover, SPID and CIE capability of securely and uniquely identifying a user can serve many purposes. For example, in high LOA identity systems, they could be

used to authenticate a client in the process of credential recovery. Moreover, the digital signature feature of SPID permits its use as a solution to sign contracts.

## 4.1. Banking sector

The Digital Era brought deep changes to the banking industry, on one side traditional banks are going through a continuous transformation process which seeks to enhance their physical assets in a world that is moving towards a digital paradigm. On the other hand the last ten years saw the birth of a new concept of bank, the digital bank, which doesn't rely on agencies and face to face interaction between firm and clients.

In order to seek as much diversity and completeness as possible, the six interviews conducted to managers of the banking industry were evenly split between three traditional and three digital banks, revealing the different approaches to digital identity management, and more specifically to onboarding, of the two categories, as shown in Table 4.1.

| Name | Digital / Traditional Banks | Customer base* | Adoption of SPID/CIE | Willingness to adopt SPID/CIE |
|---|---|---|---|---|
| Bank 1 | Traditional | 13,500 | No | No |
| Bank 2 | Traditional | 1,000 | No | No |
| Bank 3 | Traditional | 600 | No | Yes |
| Bank 4 | Digital | 350 | Yes | Yes |
| Bank 5 | Digital | 53 | No | Yes |
| Bank 6 | Digital | 200 | Yes | Yes |

* Data expressed in thousands of units

Table 4.1 - Banking industry

### 4.1.1. Onboarding in traditional banks

With a widespread presence on the local territory, traditional banks base their onboarding process on the *de visu* recognition of the client, performed in agencies distributed on the territory. This modality represents almost the totality of the identifications performed. Several players either already have or are considering implementing modalities to allow a remote banking account opening. As described by Bank 1 manager, this channel is not sponsored for all customers, since it is perceived as more attractive for young people:

> *"Surely the de visu recognition for us is a key component, we are not a digital bank, (…) nowadays we are not pushing on an online onboarding process toward the subscription of a pure digital identity, referring to the opening of a banking account or other products"*
>
> (Bank 1 manager)

However, an increasing number of traditional banks are combining face-to-face recognition with electronic procedures to identify a new customer. Regarding this latter method, the customer is asked to upload personal information together with a picture or a scan of an identity document. Then, two modalities of verification of these data could be available:

- a video-selfie, where the customer is usually requested to say a passphrase and/or show the identity document previously uploaded, in order to check the genuine presence of a real user.
- a wire transfer from another bank, using a previous identification operated by another banking institution as a security factor.

The onboarding process, regardless of what modality it gets carried out with, is a preliminary step for the creation of an internal digital identity, issued and managed by the bank itself. Banks provide every customer with a digital identity, for them to be able to conduct online operations and, in most realities, it is also needed for offline operation conducted in agencies.

As described by Bank 1 manager:

> *"We issue a digital identity that permits customers to access online channels and to sing contracts of any nature. (…) We do not accept paper contracts anymore, if a client wants to operate with us, he needs to have our digital identity. This is also needed to sign contracts in branch-office."*

(Bank 1 manager)

While considering the implementation of an online onboarding, there are concerns regarding compliance, security and regulation, that are particularly relevant for the banking industry due to the high level of criticality of their business. As a Bank 2 manager explained:

> *"One of the reasons we don't have it [the online onboarding method] right now it's precisely this: we've always wanted to open a digital channel, but in the realization phase we bumped into regulation issues. Therefore, our Compliance Office raised this point of attention on the only method we would have used, the wire transfer, basically stopping the intention to proceed."*

(Bank 2 manager)

The Bank 1 manager makes similar considerations, since compliance and legal matters are priority in the bank industry:

> *"We know potentialities of SPID and CIE, but we also know their limits. We are conscious that the current remote identification methodologies urge some innovation, we are working on finding alternative solution that are in primis compliant, because we are subject to anti-money-laundering (AML) and normative regulations, thus having a lot more constraint than non-banking companies. We are evaluating a variety of solution and SPID and CIE are some of these."*

(Bank 1 manager)

From the user experience perspective there are mixed opinions and both points of advantage and disadvantage.

From one side, the use of a secure and externally certified digital identity would result on an immediate onboarding process, which is not true for video-selfie and bank transfer that require back-office controls, leading to improved costs and a lower number of clients dropping the process. Bank 2 manager also explains as SPID could simplify onboarding on the customer side.

> *"We observe with strong interest the evolution of national digital identities such as SPID, because we consider it as an enabling factor that could facilitate the customer on the onboarding phase, considering that typically onboarding in the banking sector is much more complex than in other industries."*
>
> (Bank 2 manager)

Nevertheless, there are concerns on customers' ability to effectively use the two systems. Although the number of SPID and CIE identities issued is very high, covering 53.6% of the adult Italian population, it is not clear how many of these people are comfortable using the two solutions, and how many credentials have been lost or forgotten.

Bank 1 manager pointed out these concerns:

> *"We see journals celebrating SPID and its diffusion rate, but it is not sure how many Italians are effectively able to use it: one thing is creating a SPID account for a specific bureaucratic procedure, another is being able to use it after a long time has passed."*
>
> (Bank 1 manager)

Further concerns are relative about SPID technical maturity, mostly regarding standardization issues between IdPs and doubts on the ability of IdPs to sustain the banking industry risk level. While some actors consider SPID to be extremely secure, others are concerned about the implications and responsibility of a

successful fraud attempt, remarking that there is not such a thing as a perfectly secure system. From a different perspective, the externalization of this risk and relative responsibility might be a selling point for SPID. As Bank 1 manager pointed out:

> *"An obstacle and issue we are facing concerns the responsibility on eventual identity thefts, we are trying to understand who takes the risk of a fraudulent identification operated via SPID, because if IdPs take it the bank might have interest in moving away the risk onto another entity. It is key to understand if IdPs are able to sustain the "bank level risk", that is way superior to the one of public administrations."*
>
> (Bank 1 manager)

Summarizing, traditional banks are closely monitoring the evolution of national digital identity scenario in order to spot possible synergies in the financial sector, they know cultural and technological changes are happening and some of them are starting to implement solutions for online onboarding. SPID and CIE appear as immature but interesting tools, but a form of onboarding online does not currently represent a priority.

### 4.1.2. Onboarding on Digital Banks

Digital banks do not rely on physical agencies for their interactions with customers, being digital is a key paradigm of their business model, thus leading to a strong positive attitude towards the adoption of national digital identity systems. For a digital bank, being able to perform an online onboarding is a necessity, since all the interactions with clients take place either via app or website. As Bank 6 manager explained:

> *"For us a step into an agency is not conceived, printing paper is not in our nature, we are completely paperless, completely remote and completely digital."*
>
> (Bank 6 manager)

This type of bank addresses "digital-friendly" users, greatly impacting their willingness to explore new technologies. Digital tools and solutions are a distinctive point for digital banks, they address digitally capable customer base, that are looking for innovative and contactless solutions, resulting in a young client base.

Regarding the remote identification process, different modalities are available. Along with the previously mentioned bank transfer and video selfie, all the interviewed players already have or are in the process to implement SPID and are planning to implement recognition through CIE in the short term.

Digital banks have a strongly positive attitude regarding the national digital identity systems, especially towards SPID, while CIE is seen as a second step. Online identification systems are evaluated by companies according to three main dimensions, being: Security, Cost and User Experience. From interviews with actors that have already implemented the solution, a qualitative idea of SPID performances on these three dimensions is presented.

Security, as described by Bank 6 manager, is fundamental in the banking industry, with no exception for digital banks, and onboarding in particular is a sensitive process in those regards:

> *"We have to be sure that who we are interacting with is the person that is truly requesting for the banking account, that we are not in front of a fraud attempt or an identity theft because this process leads to the opening a very delicate relationship, such as portfolio management."*
>
> (Bank 6 manager)

Many actors consider SPID as a secure system, and as a positive factor that it was created, and sponsored by the Italian Government. this is an important strong point for SPID, especially compared to the bank transfer that carries concerns about security and compliance issues. Bank 4 manager pointed out:

> *"I'll say something that might sound trivial, but it is not, SPID can be seen as a commercial or innovation project, but it is first and foremost a security project."*
>
> (Bank 4 manager)

Also:

> *"Thanks to SPID that is performing so well, and the others remote recognition modalities, we decided to dispose of the recognition via bank transfer, in favor of more certain identification methods."*
>
> (Bank 4 manager)

Moreover, SPID greatly outperforms the identification via video-selfie or video-call in terms of costs, as described by Bank 4 manager:

> *"Web ID [video-selfie method] is absolutely the most expensive tool we have, the one that impacts the most our onboarding cost, we are talking about 25-27 € per identification, against only 0,80€ of SPID."*
>
> (Bank 4 manager)

A third dimension is user experience: the companies that have implemented the national digital identity solution observed a positive reception of it by clients. In fact, identification via SPID significantly lowers the lead time of the onboarding process. Moreover, individuals that possess it are glad of using it. An empirical indicator of this phenomenon is that, where implemented, SPID experienced a steady growth in the percentage of new customers adopting it, and quickly became the most used identification method. As Bank 6 manager described:

> *"We initially approached the market with the video-selfie, but when SPID was implemented, it immediately covered 50% of identifications, my forecast is that we will be at 60-40 soon (60% SPID and 40% other methods). Video-selfie is an appealing tool, but it is extraneous to the customer. A person that already possesses SPID credentials and uses it in its daily life knows that it is very simple to use. Why should she approach a new thing if SPID does not represent a complication?"*
>
> (Bank 6 manager)

The adoption of CIE comes as a natural step further after SPID, and addresses specific needs the companies have been facing regarding the reading of identification documents for citizens and firms. Usually, the implementation of SPID took lower effort than expected, as witnessed by Bank 4 manager, resulting in a higher inclination into starting the same process with CIE.

> *"With had no barriers in the implementation of SPID, we have a great relationship with our technology provider, and had a very fast implementation process. With SPID zero difficulties."*
>
> (Bank 4 manager)

Most of digital banks are integrating SPID as an identification modality for their onboarding process. In this process actors are usually supported by their current technology partner, by whom they are provided services as the digital signature, and that typically is a SPID IdP. As Bank 6 manager explained:

> *"We are supported by Intesa for SPID because Intesa uses SPID to provide us the digital signature, to be able to sign contracts regarding bank accounts and the onboarding procedure."*
>
> (Bank 6 manager)

Banks that already adopted SPID in their onboarding process are not registered as SPID SPs: the three IdPs that offer the digital signature though SPID - being In.Te.S.A., Namirial, and Infocert - are using a one-shot digital signature service to relieve banks form the bureaucratic procedure of registering as a SP. Thus, implying that the "official" number of SPs for SPID is slightly underestimated in relation to the real number of companies using the digital identity.

Actors have shown little to no interest in the opportunity of using SPID digital signature to sign contracts with customers, banks are satisfied with their current sign modalities and there are no pushes for change.

As Bank 5 manager pointed out:

> *"Our digital signature system will remain as it is. Moreover, our technology provider provides us with many other services where customers data are involved. Our scope as IT is to focus on what is strategic for us, where we can invest every year, and delegate elsewhere to market experts those things that do not belong to our expertise camp."*
>
> (Bank 5 manager)

Thus, technology providers, in many cases also IdP in the SPID ecosystem, have a key role in fostering the adoption of digital identity systems, both answering positively to partnering companies asking for the implementation of a new system, and sometimes even directly proposing it to managers. It is important to consider that most of the companies that adopted SPID already had other services provided by a SPID IdP, and that this factor is positively impacting its adoption in the private sector. In this regards the distributed model of SPID ecosystem presents the advantage of intermediaries being sponsors of the digital identity system, unlike in the case of CIE.

### 4.1.3. Authentication in the Banking sector

All the interviewed players of the Banking sector offer customers the possibility to authenticate to their Home Banking using a set of credentials provided and managed by the bank since the end of the onboarding process, with the possibility of using biometric identification offered by the user's device to streamline credential entry when accessing the personal area.

None of the actors uses or is considering adopting SPID or CIE as an authentication modality. From the interviews emerged that companies are satisfied by their current authentication systems. Thus, SPID and CIE do not seem to carry significative advantages such as to justify the switching and/or integration costs for their implementation.

Substantially, from this perspective there is not a significant push for innovation. As Bank 5 manager explained, banks consider their system to perform well in terms of user experience:

> *"We are not considering it, because our current authentication service is streamlined, and we don't see reasons to take any risks."*
>
> (Bank 5 manager)

Also, Bank 4 manager:

> *"After years of having these credential where everything, even our anti-fraud engine is based on our user-id and password mechanism, in which we have invested a lot, we need a really strong reason to change what we currently have."*
>
> (Bank 4 manager)

Banks sustained massive investments on their current customer personal areas and customers are used to access it with their current credentials.

Another barrier is represented by problems of a regulatory nature: as described by Bank 1 manager, the banking sectors is subject to strict standards and norms which SPID and CIE are not totally compliant to.

> *"Regarding the possibility of using SPID or CIE as an authentication method for our channels, it is a furtherly delicate theme since it is subject to several issues in matter of security and regulation. These matters have been highlighted by us and other European banks when the UE began discussing about digital identity."*
>
> (Bank 1 manager)

### 4.1.4. Further use cases

One traditional bank is in the process of implementing SPID, and plans on subsequently adopting CIE, for the purpose of credential recovery. This actor is currently not considering an adoption of SPID for onboarding or authentication purposes, since a *de visu* recognition is incentivized to create a relationship with the client. Two reasons for the adoption of SPID in this functionality have been individuated:

- give clients an easier alternative to the complex current remote password recovery modality, which is based on OTP, SMS and e-mail as authentication factors.
- complete the bureaucratic procedures and make experience with SPID and CIE, with the purpose of being prepared to further use cases of the two solutions.

Bank 2 manager explained the reasoning behind this choice:

> *"Currently our bank is not prone towards an online onboarding modality. Our function, being the IT, decided that we could not "wait and see" without experimenting these technologies. Therefore, we decided to implement it in simple use-cases to make experience."*
>
> (Bank 2 manager)

An additional insight is how the IT function oversees the scouting, studying and experimenting of new technologies, and often acts as an internal change promotor.

### 4.1.5. Conclusion

The banking industry is very active and informed about remote identification modalities, the sector is very sensitive about the matter and looks with interest towards both SPID and CIE. There is willingness to innovate in this matter, digital banks act as forerunners, driven by their need of remotely identify users. Where

SPID has been adopted for onboarding, it registered greatly positive results, both in terms of security, cost, and user experience, leading to increased trust towards national digital identity systems and encouraging the implementation of CIE.

Traditional banks are a step behind: their customer base is not as digital oriented, and the number of customers recognized at a distance is limited. Despite this, they know that at least one online onboarding modality must be made available to customers. Moreover, they look at the theme with increasing interest, innovation must be made and SPID and CIE are observed with attention.

Following, a sum-up of the main drivers and barriers emerged from the interviews:

Drivers:

- SPID greater security compared to brank transfer
- SPID decreased cost compared to video-selfie
- SPID user experience and immediacy of identification

Barriers:

- SPID unclear legal responsibility for identity theft
- Low perceived users' maturity for the use of SPID and CIE
- Switching costs and organizational adjustment
- Satisfaction with current identity management systems
- Concerns in the matter of regulation and compliance

Summarizing, while CIE and SPID are solutions that address a real, strategic, and immediate need of digital banks, traditional banks are staying a step behind, because currently innovating online onboarding is not a priority.

Regarding authentication, none of the actors is considering the adoption of SPID and CIE. An eventual implementation would have to deal with a complex integration into the current identity management system, and all the customers that are willing to use the home-banking are already successfully using it with their existing credentials. In such a regulated industry, every process involving identity

is important and costly. Consequently, a clear proposition of value is needed to push banks into investing resources.

## 4.2. Insurance sector

The Insurance sector is made up of companies that offer risk management in the form of insurance contracts, but not all the insurance companies offer the same product or cater to the same customer base.

In this regard, it is necessary to differentiate between the traditional insurance companies, with a regional presence guaranteed by agencies and agents on the territory, and that offer a variety of insurance services spacing such as life, health, property and accident insurance, from the online insurances, that usually focus on services with relatively less critical nature, such as property and accident insurance for vehicles, and manage all the transactions with users on the online channel. Below (Table 4.2) an overview of the interviewed firms.

| Name | Online / Traditional Insurance | Customer base* | Adoption of SPID/CIE | Willingness to adopt SPID/CIE |
|---|---|---|---|---|
| Insurance 1 | Traditional | 3,500 | No | No |
| Insurance 2 | Traditional | 1,000 | No | Yes |
| Insurance 3 | Traditional | 60 | No | No |
| Insurance 4 | Online | 650 | No | No |
| Insurance 5 | Online | 450 | No | No |

* Data expressed in thousands of units

Table 4.2 - Insurance industry

Life insurance, which is a contract that offers financial compensation in case of death or disability, must be considered with particular attention, since it requires by regulation a high LOA for the identification process and an in-depth interview with the client. This is not true for any other type of insurance.

### 4.2.1. Onboarding on online insurance companies

This second typology of insurance company bases its business mainly on non-life insurances, that will be referred from now on as "general insurances", mostly car insurance, which is mandatory in Italy, and is referred to a price-sensitive customer base. The onboarding procedure usually ends with the new customer purchasing a product and the interaction between clients and company are limited to the minimum. As Insurance 5 manager explained:

> *"For an insurance company of our kind, the identification of the client is not a highly critical process, for us the issuing of an insurance is a basic process, meaning that currently our main product is car insurance, where the client hopes to use our systems once a year, when its product expires."*
>
> (Insurance 5 manager)

For this category, the website is the main onboarding channel. The user accesses the website and creates a quotation by inserting its personal data and selecting the desired product. The process ends with the customer that is given credentials to access its personal area and completes the purchase of the insurance within the website.

The initial phase of onboarding that leads to the creation of a quotation can also happen via phone or through third party aggregators. Nevertheless, the customer is then redirected to the company website.

In this process several verifications on personal data entered by the customer are performed, specifically its email address and/or telephone number are verified through OTP or magic link. These verifications are aimed to establish a secure

communication channel with the customer through the creation of a personal area, mandatory for sector regulation.

Regarding car insurance, all the insurance companies collect customer related data though a national database, provided by ANIA, the Italian national association of insurance companies (Associazione Nazionale fra le Imprese Assicuratrici), which is freely accessible by registered insurances. The information gathered through ANIA database is used to make the estimate of the cost of the policy to customers. Therefore, clients are not asked further forms of identity verification in this phase.

As Insurance 5 manager explained:

> *"To release our core business, that is car insurance, for us it is sufficient to have a license plate and a birth date. With these data we have access to ANIA database (…), where all owner data are registered. Thus, we are not demanded to ask anything to the customer because we have lots of information, such as personal data, how many years he has been a policy holder and if he had accidents."*
>
> (Insurance 5 manager)

Also, from Insurance 4 manager:

> *"If customer's declared data match with those gathered from the external database, the flow of making a quotation becomes very simplified. There is no need to ask any input to clients because we gather those data externally."*
>
> (Insurance 4 manager)

Therefore, the issuance of general insurances does not require a high LOA verification of personal data, and the focus - in the onboarding process - is providing the customer with a process as streamlined and simple as possible. This represents a barrier for the adoption of SPID and CIE for this purpose, as Insurance 4 manager explained:

*"SPID has a multi-factor authentication by design, this might be a benefit but is also a constraint, because a multi-factor authentication surely represents a point of strength from a security point of view, but also a complication for user authentication in a website, especially if the service accessed through this authentication does not require a sensitivity level such as to justify this complexity. This may represent an important downside from the user experience point of view."*

(Insurance 4 manager)

Moreover, there is not a significative push to innovation in this matter. The actual cost of onboarding is very low – given the weak checks carried out on the identity of the user – and a potential further investment appears unjustified by the criticality of the process, as Insurance 5 manager pointed out:

*"For us, customers' recognition, and the onboarding in general, until we manage to add other services apart from car insurance, as we have intention to, it is currently a no-return investment."*

(Insurance 5 manager)

### 4.2.2. Onboarding on traditional insurance companies

Traditional insurance companies have a direct contact with the customer, they offer a wide variety of insurance products and rely on agents to maintain a relationship with clients. For such reasons, as explained by Insurance 1 manager, not many companies have an online onboarding procedure:

*"Our company chose at policy level to be agent-centric, meaning that the relationship with the client is based upon trust and encounter. Thus, we use digital tools for a first approach, but there is not such a thing as a full digital onboarding."*

(Insurance 1 manager)

In the case of life insurances, an investigation on clients' economic, family, social and sanitary status is required by law and the regulation authority.

Nevertheless, also in the case of general insurances, traditional insurances gather a lot of information from their clients. This approach is in line with the business model of these companies, since traditional insurances average customer holds a multitude of policies tailored on its needs.

Thus, agents seek for a deeper understanding of customers:

> *"The agent is that person who knows the customer and is able to make up-selling and cross-selling, thing that is very difficult to approach in a centralised way."*
>
> (Insurance 2 manager)

Also, Insurance 1 manager:

> *"We collect a great amount of data. Starting from extended personal data, including its family members because, for example, its insurance needs depend on him having or not having kids."*
>
> (Insurance 1 manager)

All insurance companies provide customers with a personal online area, but most insurance companies are not investing in it. The reason behind the lack of interest in these matters stands on a low expected return on investments: traditionally this solution serves mainly the purpose of consultation rather than enabling action since customers do not access their home insurance frequently.

As pointed out by Insurance 3 manager:

> *"While you access home banking very often, for home insurance is a different kind of business, you only access it once or twice a year, so there is a cost/benefit issue to be evaluated. How much does this cost to me? If the client uses it twice a year, is it worth to invest?"*
>
> (Insurance 3 manager)

An analogue argument is valid for user identification: the very first recognition of a client is conducted *de visu* by agents, and customers rarely carry out operations online.

As Insurance 1 manager explained:

> *"In my opinion the main barrier is that currently identification is not seen as a critical process that impacts on business growth?"*
>
> (Insurance 1 manager)

Recently, some companies have undergone a process of innovation and digitalization, with the aim of enabling customers to perform different actions online, without the intermediation of an agent. Insurance manager 2 explained how in the online channel can be beneficial for the client to manage some type of low added value services, that do not require agents counselling to be carried out.

> *"Online tools are super useful when the client needs a service, for example in case of accident, where the agent is not really interested in managing the thing since his compensation depends on policies selling. If a client is able to carry out the claim in less than 24h, he will probably remain your customer for at least 15 years."*
>
> (Insurance 2 manager)

On the other hand, the use of a centralised channel for CRM purposes, or for the offering of a policy, could be negatively received by agents, as they would feel cut off. For these reasons, it is fundamental to strike a balance and act with delicacy in exploiting these opportunities.

> *"There are two kinds of agents: on one side there are those that are happy to have new customers coming from the web channel and are confident in using the smartphone app to communicate and sign contracts with their clients.*
>
> *On the other side there is the agent that does not want the company to send email to their customer pool, or to propose things that he does not*

*think to be in line with his customer needs. Those are the old-style kind of agents."*

(Insurance 2 manager)

Moreover, the lockdowns caused by the global pandemic have played a role in studying and pushing for online solutions, as Insurance 2 manager explained:

*"The necessity was born with Covid, at the first lockdown we've been asking ourselves – what do we do now? – then we started implementing online purchasing tools."*

(Insurance 2 manager)

A real online identification is performed for actions that require a higher LOA, such as in the case of a life insurance, or when a customer wants to dispose a critical request from its personal area. In these cases, a supplementary recognition phase is needed, where the customer is usually asked for a face-picture and an identification document. Alternatively, the process can be carried out via call-center.

One interviewed company is implementing SPID to complement the current online identification modality. The adoption proposal came from its technology provider, that is a SPID IdP, and already assisted them in the implementation of their current online identification solution. Simplicity of SPID and its great diffusion have been pointed out as its main points of strength, and the main driver is user experience.

This first adoption will be followed by further use-modalities for SPID, underlying as a triggering factor can act as a forerunner for further use cases.

As Insurance 2 manager explained:

*"We are substituting our identification tool with SPID, the simplest tool, isn't it? Our technology provider recently proposed to us this opportunity."*

(Insurance 2 manager)

And also:

> *"My first concern is to provide a tool as simple as possible, and SPID is becoming a common system in Italy. I will implement it wherever it is possible, starting from registration to home insurance, because that is a process that often leads to problems for customers."*
>
> (Insurance 2 manager)

This remarks the key role of technology providers in the developing of these solutions also for Insurance sector: often the push for SPID adoption comes from IdPs and their relationships with their business partners.

### 4.2.3. Conclusion

Online insurance companies have a simple identification process, which has a negligible cost for the organization, while SPID has a fee that must be paid to IdPs for identifications. For this type of insurance there is no reason to pay SPID for a higher LOA when it is not required for the process, resulting in a very low interest and adoption inclination.

On the other side, currently most of traditional insurances do not offer an online onboarding procedure, mainly because their entire business model is based on agents and their ability to relate with customers. Some insurances have implemented some identification method, in a post-onboarding phase, to allow customers to perform specific actions in their "home insurance", and SPID or CIE could address this need.

Following, a sum-up of the main drivers and barriers emerged from the interviews:

Drivers:

- SPID simplicity and diffusion
- Support from technology provider for SPID implementation

Barriers:

- Low utilization rate of personal area
- Low criticality of identification for general insurance purposes
- Switching costs and organizational adjustment

The main barriers depend on the tradeoff between value and costs. The insurance industry results difficult to attack, without either improving the value proposition of SPID and CIE, or by restructuring integration and utilization costs for the two systems.

## 4.3. Utility sector

Companies in the utility sector mostly rely on a network of intermediaries and agencies deployed on the territory for customer's onboarding and relationship management. Another traditional channel of acquisition is via telephone. Nevertheless, there is an ongoing innovative drive towards the online channel and digitalization of utility onboarding and service. For this sector, four companies have been interviewed (Table 4.3).

| Name | Digital / Traditional Utility | Customer base* | Adoption of SPID/CIE | Willingness to adopt SPID/CIE |
|---|---|---|---|---|
| Utility 1 | Traditional | 180 | No | No |
| Utility 2 | Traditional | 1,600 | No | Yes |
| Utility 3 | Digital | 8 | Yes | Yes |
| Utility 4 | Digital | 150 | No | No |

* Data expressed in thousands of units

Table 4.3 – Utility industry

### 4.3.1. Onboarding on utility companies

The online onboarding is usually performed through the compilation of an online form on the website. During this process personal data of the customer are collected, alongside technical data regarding the electric and/or gas supply and payment information. Some companies in this process require customers to upload a picture of themselves and an identification document, some others favor a streamlined process to not impact user experience and trust clients' data. The process ends with the signature of the contract via OTP.

Before the contract is signed, a credit check is carried out on the payment information provided by the customer: this check has a double purpose, aside from ensuring the financial position of the customer it allows a first form of trusted identification. As Utility 3 manager explained:

> *"Through a system called check-Iban, we discover if that Iban is associated with the personal number provided by the customer, thus getting possession of its demographic information, and a further confirmation that the given Iban is entitled with the customer. We take for granted that a person manages to open a banking account only if the bank verified its identity."*
>
> (Utility 3 manager)

Utility companies are particularly sensitive about the tradeoff between identification LOA and user experience. In these regards SPID is perceived as a valid alternative to the current identification and data collection procedures. Moreover, the form filling operated by customers is clearly prone to compilation mistakes and fraud attempts, raising issues about compliance and regulation. Call-center is often used to overcome this problem: some companies use it proactively, and the call by an operator is scheduled in the onboarding process, some others use it reactively, to solve issues when provided and collected data do not match.

Therefore, SPID is appealing for three reasons:

- firstly, it provides certified information, with a strong legal and factual reliability.
- it could save costs if substituting the use of an expensive tool, being the call-center.
- it can enhance the user experience, streamlining some actions, such as the upload of selfie and documents by the customer.

As Utility 2 manager explained:

> *"We started talking with business about a potential adoption of SPID, because it carries within a series of certified information. This potentially could permit to avoid the intervention of the call center in the pre-acquisition phase, currently carried out for documents and personal data validation."*
>
> (Utility 2 manager)

From the legal point of view, the main driver for the adoption of SPID is the possibility of using it to sign contacts, even if there are doubts about the legal maturity of this service. Digital signature on SPID is a new feature and it is offered by only two IdPs, generating concerns about compliance and standardization.

Indeed, Utility 4 manager pointed out:

> *"SPID would solve the onboarding problem because it could substitute the current sign system thanks to its digital signature feature, even if I carry some doubts from the legal point of view."*
>
> (Utility 4 manager)

In terms of data acquisition, an interviewed player has implemented SPID in its onboarding process, particularly not in the identification phase, but after the contract is signed. In fact, SPID is necessary to access a public database that contains

citizens data about utility goods consumption, provided by ARERA, (Autorità di Regolazione per Energia, Reti e Ambiente; Regulatory Authority for Energy, Networks and Environment). The mentioned utility firm operates a check to understand if the new customer is or is not in possess of a SPID identity. If the check has a positive response, the customer is asked to access the database and give access to those data. This specific company offers fixed-rate fees, as opposed to the market standard that applies fee based on the real consumption of customers. For this reason, accurately predicting clients' consumption is fundamental in achieving an economic advantage, both for customers and the firm. If the customer does not possess a SPID identity, it is proposed to create it, with the offer by the utility company of bearing the costs of this process.

As Utility 3 manager explained:

> *"For our business model it is fundamental to know the real consumption of customers, before deciding if being or not their provider. The only way to know these data in advance is to access the consumption portal and collect this information."*
>
> (Utility 3 manager)

This use case displays the potential and not expressed value of systems such as SPID and CIE. This company needs to gather information from a third-party database so much that it is willing to pay SPID registration to the customer in order to access those data. Nonetheless, this process of the customer sharing those data today is conducted manually, with him having to access the database, collect those data and sending them to the company. The possibility of using SPID and CIE to enable firms to directly perform operation with customer's consent on third parties' platforms could greatly enhance national digital identity systems value proposition.

Moreover, as Utility 3 manager suggested, a further way to enhance SPID and CIE value proposition could be the enrichment of accessible data:

> *"My wish for SPID is to have, with a single access, the possibility to choose to what information get access (…). I imagine the possibility of a*

*SPID user that possesses a series of already registered information in its digital identity, which I can access easily with its authorization."*

(Utility 3 manager)

Looking at CIE, none of the actors have any intention to implement it. As Utility 3 manager explains, the need it addresses, being able to recognize an identification document, is not critical for the utility sector, which does not strictly need a high LOA identification at compliance level.

*"From a legal point of view, having the identification document of a customer does not give me any guarantee. In the moment I have the contract signed, paid and concluded, I do not have any legal constraint to memorize, collect and store customers' identification document."*

(Utility 3 manager)

### 4.3.2. User authentication

Utility companies usually provide customers with an online personal area, which, however, it is not mandatory for the user to activate. Depending on the digitalization level of the company and therefore on its customer base, this tool features different levels of criticality from firm to firm. In most cases, the utilization rate of personal area by customers is very low, limiting firms' willingness to invest in this matter. As Utility 4 manager pointed out:

*"I think around 60% of our customers activate their self-care account. And even for this 60% accesses are very low; people don't care about logging in their personal area."*

(Utility 4 manager)

Adoption of SPID is perceived to carry many advantages, especially in terms of user experience. Anyway, innovation of authentication methods is not a priority for most utility companies, and these kinds of projects remain long-term intentions.

In these regards, Utility 4 manager said:

> *"Finally, SPID reached a wide diffusion, and I am certain that in some time it will take off, because it really is convenient, especially with Poste Italiane App. I'm very passionate about this, moreover I'd like to get rid of these passwords, that are a problem for everybody."*
>
> (Utility 4 manager)

### 4.3.3. Conclusion

The utility industry presents a discrete propension toward the adoption of external digital identity systems, supported by a certain degree of flexibility in terms of regulation of the market. However, the perceived value of SPID and CIE remains notional, and struggles to trigger an action for adoption. In fact, this industry does not require a high LOA identification and, moreover, the rate of use of the personal area is very low.

Following, a sum-up of the main drivers and barriers emerged from the interviews.

Drivers:

- SPID as an alternative to call-center
- SPID as a security solution
- SPID and CIE offer great legal guarantees
- SPID as an access key for customer's energy consumptions
- SPID user experience
- SPID as a signing solution

Barriers:

- Low utilization rate of personal area
- Low criticality of identification
- Switching costs and organizational adjustment
- Willingness to directly manage internal digital identity

## 4.4. CIE is a step behind

The biggest insight that comes as a result of this research is the difference of interested showed by the interviewees towards the two different national digital identity systems, SPID and CIE. Despite the numbers of the two solutions are similar - with 26.1 million identities issued for SPID[34] against the 24.7 of CIE[35] at the date of October 2021 - SPID appears significantly more appealing to the private sector. Out of the 15 interviewed companies, none already implemented CIE, and, in those case where a future implementation is planned, SPID is already adopted, with CIE coming as a second step.

Going into detail, for CIE four possible use cases have been observed during the research, all retrieved during interviews with managers from the banking industry:

- online identification and data acquisition for onboarding purposes.
- customers' data acquisition, performed in agency with an NFC reader, with the objective of obtaining a high-quality picture and avoid typing errors.
- credential retrieval, to simplify complex password and credential recovery processes.
- step-up authentication, as a security element to enable online operations at high criticality.

[34] https://avanzamentodigitale.italia.it/it
[35] https://www.cartaidentita.interno.gov.it/en/home/

Companies have only recently started to approach national digital identity systems, with most of SPID and CIE adoptions on users' side registered in 2021. SPID and CIE are two different solutions, but in most cases they serve the same purpose, being retrieving customers' information in the online onboarding process. Moreover, the implementations of SPID and CIE do not happen in the same project, and thus a choice must be made between the two solutions.

Summarising, besides specific uses that require the reading of an identification document, a choice must be made between SPID and CIE, and SPID happens to be favourited, for several reasons.

First and foremost, SPID is more widespread. Even if numbers of issued credential between the two solutions are comparable, most part of CIE owners use it as a traditional identification document. SPID, on the other side, serves the only purpose of being a digital identity system, has been strongly supported by initiatives of the Italian government, and has wider media coverage. Moreover, many managers used SPID in their private life as users, and experienced in first person its ease of use, as described by Insurance 1 manager:

> *"I have used SPID, I've registered recently, and it is incredibly easy, I only have to memorize one password and it is super-fast"*
>
> (Insurance 1 manager)

SPID being more widespread and mature as a digital solution is also reflected in the difference between the numbers of public and private SPs of the two systems. Table 4.4 shows detailed information about SPID[36] and CIE[37] at the date of October 2021.

| | **Public SPs** | **Private SPs** |
|---|---|---|
| **SPID** | 9,801 | 59 |
| **CIE** | 1,790 | 3 |

Table 4.4 – CIE & SPID SPs comparison

[36] https://avanzamentodigitale.italia.it/it
[37] https://federazione.servizicie.interno.gov.it/listSP

Another point of advantage for SPID is represented by its IdPs. In fact, a great part of SPID IdPs provides companies in the analyzed sectors with technological services and digital products, such as digital signature and certified e-mail. The analysis of the interviews showed how IdPs proposed and conducted projects regarding SPID implementation and diffusion among SPs, and how, thanks to their commitment, these adoption projects advanced in a flowless way. On the other side, CIE does not dispose of a network of IdPs to push its adoption.

Moreover, NFC technology is required to use CIE, that is the main differentiation point from SPID and in specific contexts represents an advantage, for remote onboarding purposes may constitute a barrier.

A remote reading of a CIE must be operated through an NFC dispositive in possess of the user, usually a smartphone. As Bank 1 manager pointed out, this may raise concerns, primarily about the presence of the technology on client's device, and furthermore on the security level and protocols of each different device:

> *"For what concerns the electronic identity card, there is a technological difficulty withing the use of NFC on smartphones, for the vast assortment of devices on the market, all of them with different standards. Moreover, NFC can only be used on its native app, meaning that customers must download that app, thing that is not always easy to apply during an onboarding process."*
>
> (Bank 1 manager)

## 4.5. The authentication problem

The analysis of these interviews showed a positive consideration for the national digital identity systems taken in exam, especially for SPID, with many of the companies involved having already implemented the solution or being on the point of implementing it. Companies are interested in using SPID to collect verified and compliant data about their customers with the aim of inputting those data in their

own identity management system. Anyway, none of these adoptions considered a use case for authentication purposes, and for a variety of reasons, with differences among the investigated sectors.

In the bank industry, personal areas are significantly utilized by users, and the nature of operations conducted requires a high LOA system, characteristics that should incentivize an adoption of SPID for authentication purposes. Nevertheless, while the implementation of SPID for online onboarding processes addressed a specific need and comes into play in a relatively recent process, banks have been providing home banking services for years, thus developing, updating, and maintaining compliant identity management systems. An adoption of SPID or CIE, for authentication purposes, would not deliver any advantages over the current systems in use, as Bank 1 manager explained:

> *"Regulations, as in the case of PSD2, forced banks to adapt and provide authentication modalities very similar to SPID, and does not make any sense to start over with a new system, also because in that case customers would have to adapt as well. Bank credentials are some of the few that customers know how to use and preserve, because investments have been made on this matter."*
>
> (Bank 1 manager)

For the insurance and utility industry the topic is quite different, mainly for a lower level of LOA in the authentication process, and for a limited use by customers of their personal areas, that impacts on priority and magnitude of possible investments. The low usage of customer personal areas, on the other side, constitutes a possible point of advantage for SPID: utility and insurance companies have problems regarding the ability of customers to retain credentials they use once or twice a year, as Insurance 5 manager explained:

> *"Happens that those customers that did not have accidents, after one year have to renew their car insurance and do not remember their password"*
>
> (Insurance 5 manager)

Also, from Utility 4 manager:

> *"SPID could be a great login system, solving a lot of issues customers have. Instead of creating the hundredth password, that everybody knows how easy it is to forget or to be used cross-platform, SPID could be used as an authentication system. I am a fan of the password-less paradigm."*
>
> (Utility 4 manager)

Nevertheless, in most cases the tradeoff between expected costs and benefits does not favor an adoption for an external authentication method, or at least not strong enough to justify an effort for change, as Insurance 4 manager described discussing of the opportunity of implementing a social login:

> *"There have not been factors able to justify a change in authentication methodology. A change represents a cost, especially in terms of integration. (…) There are a variety of solutions offering fees with a price per authentication, not having significant benefits such as to justify a change in technology, we decided to currently do not implement any."*
>
> (Insurance 4 manager)

Summarizing, there is not a significant push for the adoption of either SPID or CIE for pure authentication purposes. Nonetheless, companies which already implemented SPID or CIE for the onboarding phase, would face less barriers for an eventual extension of their use in the authentication phase. In these regards, it must be considered that the sector which is up ahead for the implementation of the two solutions – the bank industry – is the least interested in using them for authentication and, accordingly, the opposite is true for both the insurance and utility industries.

## 4.6. Perception of SPID in the private sector

The analysis of the interviews exposed many drivers for the adoption of SPID, mainly regarding improvements in terms of cost, user experience, security and compliance, especially for the onboarding and authentication phases, and drivers related to SPID "features", such as digital signature, or the possibility to access external database with certified information about the customers.

However, the companies who already implemented SPID at the time of the interviews were a minority, being two digital banks and one utility company.

Private SPs of SPID are growing, but at a significantly lower pace if compared to its diffusion among final users. Many companies do not consider the adoption of SPID as a possibility, both for the lack of external stimuli and because, as Utility 2 manager explained, SPID and CIE have been often perceived as solution only related to the Public Administration.

> *"Initially it has been perceived by us as something made for the PA, and only recently we understood that it can be a service for private companies. Probably the roadmap followed by the PA, and its initial value proposition, made us think that it was focused on publics services, that it could not be a business service."*
>
> (Utility 2 manager)

The perception of SPID and CIE as a public-only solution is due to multitude of factors, such as:

- spot initiatives promoted by the government for SPID and CIE diffusion were related to public services.
- the vast majority of uses of SPID and CIE by citizens is made to interact with public SPs.
- the IdP that provides more than 80% of SPID identities, being Poste Italiane, is a public company.

From this point of view, the adoptions of SPID by actors of the bank industry happened during 2021 could represent a turning point, since they represent a reference point for firms of all industries, as Utility 4 manager explained:

> *"Regarding the digital paradigm, banks are really becoming a reference point, with impressive digitalization numbers. I am sure that they could act as driving forces also for other industries, such as in the case of utility, that are less responsive in these matters."*
>
> (Utility 4 manager)

Thus, suggesting how the implementation of SPID by prominent actors of the private world could lead to a domino effect for competition and imitation dynamics.

## 4.7. Suggested evolution: enrich the set of identity data

The main barrier for SPID and CIE, on those companies that considered the adoption, stands on a low perceived value that a possible implementation could lead to, especially on those industries where a high LOA identification is not a priority. For traditional banks, online onboarding represents a very small percentage of their customers acquisitions and are not interested in external authentication solutions. Digital banks, on the opposite, are a relatively new reality and strongly rely on digital onboarding to expand their customer base. In this latter segment, SPID is successful because addresses a core need, in a core process, and in a better way if compared to its alternatives.

Online insurances and utility companies do not need the high LOA offered by SPID, and whenever SPID is recognized to have advantages, they are rarely such impactful to trigger an actual adoption.

The single utility firm that already implemented SPID is not using it to collect certified demographic data of customers, but it needs SPID to access further data of technical nature present on an external national database.

Since SPID provides data that companies already have made arrangements to obtain, managers suggested that an enrichment of data obtainable through SPID could enhance its value proposition, either by expanding the set of data a user can store into its digital identity, or by using SPID as a proof of consent to share data across firms. As Insurance 4 manager explained:

> *"We are hungry for data, as all companies are, and we are even more hungry for certified data, because they allow us to simplify life for users and give us more certainties on subjects and on their non-contractual attributes. We would take advantage from external sources of data."*
>
> (Insurance 4 manager)

Utility 3 manager expresses similar thoughts, but extending the concept to sector-specific technical data:

> *"My want is, with a single SPID access, to decide what information ask to the client, so that if I am an energetic supplier, and inside a client SPID there are information regarding energetic market, I can access those without gathering them from a thousand different places. (…) I imagine the possibility where the client owns SPID and, for some public utility services, he has a series of pre-packed data I can access easily with his consent."*
>
> (Utility 3 manager)

Following this path, SPID could act as an intermediator for the sharing of certified data between firms and citizens. Banks would be interested in sharing and receiving credit information, and all those data that could simplify procedures for Know Your Customer processes. Insurances might retrieve sensible data on clients, with their consent, that would lead to a better definition of customer's risk profile, with benefits for both sides. Similarly utility companies could retrieve data on energetic consumptions and technical or personal information about their customers.

## 4.8. Organizational governance of end-users' digital identity

All the companies in the banking, insurance and utility industries offer a personal area to customers, and therefore have a digital identity management system. The decision of implementing either SPID or CIE would represent an innovation of the current identity system. The main functions involved in this decision are four, being: IT, Marketing, Security, Compliance & Legal, and specifically for banks, the AML function.

- The IT oversees the technological management of identity systems, its maintenance and evolution and is in charge of scouting for innovation in the technological field, including digital identity.
- Marketing is the function that manages the relation with clients and is involved in the decision regarding new onboarding or access modalities. Its focus is on customer user experience.
- Security monitors client's data and is in charge of detecting and avoiding fraud attempts.
- Compliance & Legal assess conformity of identity management systems to the current standards set by regulatory authorities.

Push for innovation in matter of digital identity comes for different reasons by different functions, usually IT and marketing act as promoters for change, while security and compliance & legal evaluate if the solution is compliant to their standards, and eventually veto the proposal. As Bank 1 manager described:

> *"The functions that are involved in these aspects are surely security, legal, compliance and, since we are a bank, also AML for the onboarding. The marketing is usually who makes the proposal, but the OK must come from all the mentioned functions for their area of competence."*
>
> (Bank 1 manager)

Moreover, the decision-making process is influenced by the magnitude and maturity of the organizational structure of the company, since it influences how functions interact between each other. Bank 5 manager explained these mechanics:

> *"This is and organizational and cultural theme, we are a reality of 700 employers, not 7.000, when something that creates value for the bank is to be decided, since the order of complexity is small, the decision-making process is very fast. On the opposite, in larger realities structures are more distant, dialogue is more complex, and functions may not be inclined in taking risks."*
>
> (Bank 5 manager)

Accordingly, big companies might present more resistances to the adoption of new systems, such SPID and CIE. It happens that smaller realities act as forerunners and, once barriers regarding compliance, legal, and security matters have been broken down, bigger realities will implement the solution.

## 4.9. European Digital Wallet

In June 2021, the European Commission proposed a revision[38] of eIDAS regulation, together with the presentation of the project for the creation of an informatic system for the unified gathering of documents of citizens in the European Union. This system, named European Digital Wallet, will be the conjunction of the national digital identity solutions introduced by EU member states, such as SPID and CIE for the Italian case.

[38] European Commission (2021). Proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281)

This wallet will permit citizens to share their qualified and unqualified attributes with people and companies, the validation of their personal data through a high LOA and protecting users' information in terms of privacy and sharing consent.

Even if little is known so far about this solution, a European Digital Wallet would permit customers and companies to exchange data in a secure and simple way. For firms, data are extremely important, especially regarding the Know Your Customer process but, as Insurance 3 manager pointed out, most companies would prefer an enrichment of SPID and CIE functionalities in that direction, rather than a distant European solution.

Insurance 3 manager:

> *"An Italian version would be easier, we do not have international customers, why should I connect to the European Wallet rather than to the national one? What does the European system do better?"*
>
> (Insurance 3 manager)

Accordingly, the companies interested in a European Digital Wallet are those characterized by a consistent portion of their clients residing abroad. Nevertheless, most of the companies in the utility and insurance industry in Italy operate with citizens resident in Italy only, thus finding little to no use for a European solution. As Utility 4 manager pointed out:

> *"A European Wallet If done properly would be a great solution, but not for the utility industry, that only operates with Italian people."*
>
> (Utility 4 manager)

On the other side, the banking industry operates on the international market, with international customers, even if they are usually a limited portion of the customer base.

As Bank 1 manager described:

> *"Our bank could surely be interested in using the European Wallet to recognize clients and obtain a variety of information, shorten onboarding lead time and obtain additional data. Nevertheless, we mostly operate on the national territory, and we often acquire customers with mechanics different from onboarding, thus making this wallet an advantage, but not particularly important."*
>
> (Bank 1 manager)

However, a set of certified information on European citizens is attractive, especially regarding identity documents that differ from the Italian Electronic Identity Card (CIE). Moreover, such a Wallet could interact and substitute the private alternatives offered by international Big Tech companies, by the enrichment of its proposition with payment information, simplifying the interaction between firms and customers through a public solution.

As Bank 4 manager suggested:

> *"It would be great to create a joint between the digital identity systems and customers information contained in Google and Apple wallets, of course guaranteeing a high security level."*
>
> (Bank 4 manager)

Moreover, a European Digital Wallet presents a great advantage in its public and communitarian nature, not having to relate to profit-oriented logics inherent of private companies. As Utility 2 manager pointed out:

> *"A system managed by a public entity, that does not have interests in how many times you have authenticated and in which website, from a privacy point of view would constitute a step forward."*
>
> (Utility 2 manager)

Banks would be interested in taking part of a Digital Wallet ecosystem both as users, and as data providers. Banking credentials are the most developed and used form of high LOA private digital identity in Italy. Manager of Bank 1 suggested these credentials to constitute the base of a Digital Wallet. Moreover, such a system should provide some form or economic remuneration for providing data to the system.

Bank 1 manager:

> *"Every bank developed its identity system, with important investments, also due to PSD2 regulation. This work cannot be wasted, banking credential should remain central in such a system. To make sure that banks will share their data externally, credentials so laboriously have been created, an economic convenience must be granted."*
>
> (Bank 1 manager)

Summarizing, most of the companies in the insurance and utility industries operate with a national customer base, and therefore do not see advantages is a European solution if compared to a national alternative. The banking industry has moderate interest in joining a European identity wallet, both as data users and providers of a specific digital identity certificate. Banks have sustained great investments on their identity systems; therefore, they are more interested in valorizing their current system rather than finding alternatives.

# 5 Conclusion

The objective of this chapter is to present solutions and guidelines on how to successfully enable the adoption of national digital identity systems among private service providers. These considerations are based on the insights extracted from the analysis presented in chapter 4. Thus, solutions are meant to address barriers and leverage on adoption drivers that the interviewed managers themselves pointed out.

## 5.1. Enhancing cost-benefit tradeoff

From the analysis of the interviews emerged that several barriers of different natures contributed to holding back the adoption of SPID and CIE in the banking industry. While this is partially true for the insurance and utility sector as well, it can also be stated that most barriers in the latter two industries are related to the cost-benefit tradeoff not favoring SPID and CIE adoption.

Benefits wise, managers themselves identified the enrichment of attributes accessible through the national digital identities, as the most interesting paths to enhance the value of SPID and CIE. The key advantage of a high LOA digital identity is permitting firm to know exactly who they are interacting with. Currently SPID and CIE are missing the opportunity of allowing customers to enrich their digital identity with both self-asserted and certified data to be shared with

companies. A feature that would greatly enhance SPID and CIE value proposition among citizens and firms operating in several industries.

Cost wise, utility and insurance industries showed to be way more sensible to the theme in comparison to the banking sector. All the interaction with customers performed by utility companies, and most interactions of insurance companies as well, do not require the LOA that characterizes level 3 SPID and CIE identification. In fact, for these companies a multi-factor authentication represents a barrier in term of user experience. For this reason, firms in these industries would be more interested in making use of a level 1 SPID. However, costs for the implementation of SPID and fees for its usage appear to be too expensive for firms to inspire adoption. Accordingly, some actions should be taken in these regards, with two non-mutually exclusive possibilities:

- Facilitate the implementation of SPID
- Reduce or nullify the fees for level 1 SPID usage

SPID implementation can be facilitated on two sides.

1. From a technological point of view, through the development of integration libraries and Software Development Kits (SDK). These solutions could help the implementing company on the informatic installation and integration of SPID with the pre-existent IDM.
2. From an administrative point of view, moving part of the administrative burden from companies to IdPs, through incentives or regulation. For example, some IdPs already use the expedient of running a one-shot digital signature service to relieve banks form the bureaucratic procedure of registering as a SP.

Moreover, an adjustment of the economic model of SPID featuring the elimination of usage fees for level 1 SPID, either temporary or definitive, would greatly impact on the perception of the tool by companies of several industries. This will hopefully lead to a significant increase in adoption for the solution.

Simplifications and incentives for and early adoption of SPID and CIE are crucial to reach an initial critical mass of adoption of private SPs, that would result in the following virtuous cycle (Figure 5.1).

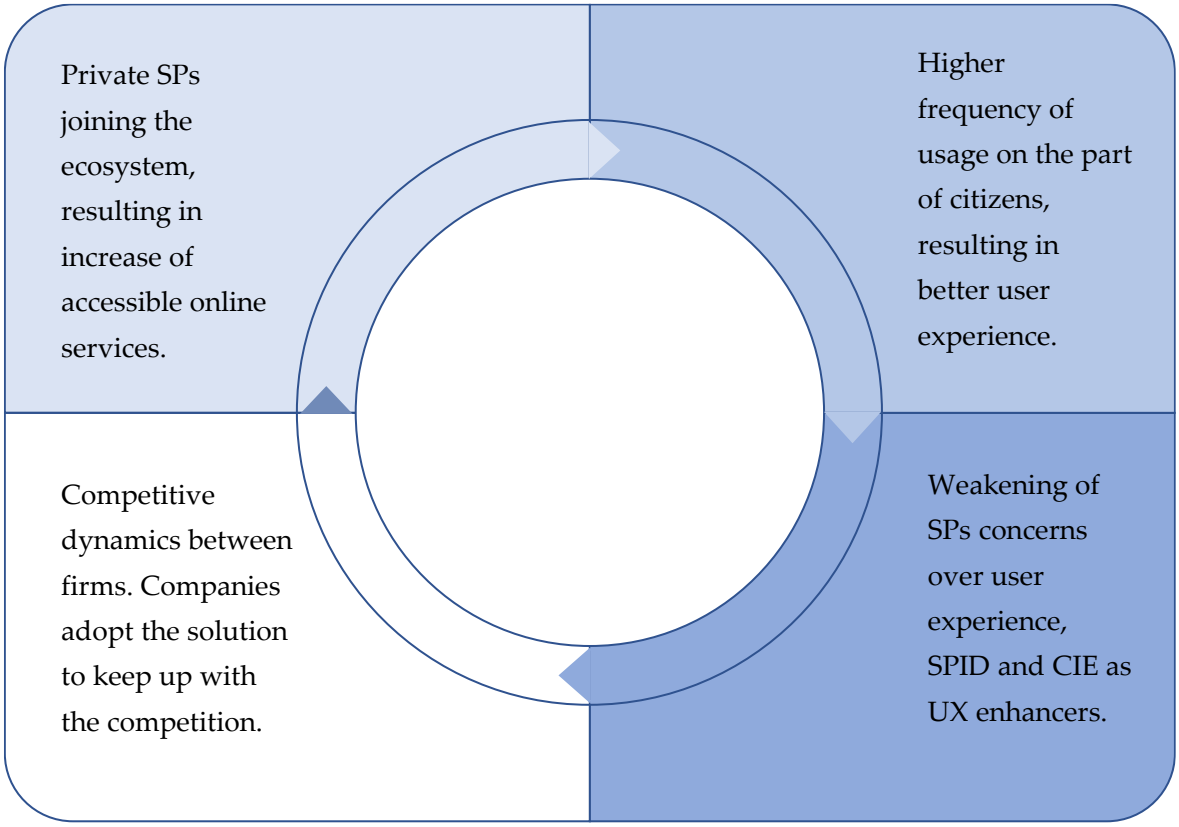



Figure 5.1 – Ecosystem growth virtuous cycle

## 5.2. Solving regulation and integration concerns

The high LOA identification featured by SPID and CIE is very attractive for the banking industry, as well as for traditional insurance companies. Especially for banks, the recognition of users is a critical process for which they are willing to invest. In this sector, fees and costs related to SPID are not the main barrier for adoption, and other factors are holding back investments in these regards.

Some actors of the banking industry showed concerns on SPID and CIE from a regulatory perspective, questioning whether these systems security and privacy protocols were compliant to the Italian and European legislations imposed by regulatory authorities. Another concern regarded the division of responsibility between SP and IdP in the recognition process in case of frauds, such as identity theft. A clear stance on the validity of these solution for identification in the banking industry, as well with a clear regulatory framework, are necessary to address these uncertainties and remove these barriers.

A further theme that emerged is about a lack of standardization. The involvement of 9 IdPs led to a certain degree of differentiation in several processes, such as pricing and the methodology used to identify citizens, and availability of ancillary services, as happens for the electronic signature. The absence of standardization generates concerns on the system stability. Moreover, it represents a barrier for those actors that are willing to implement the solution to benefit from the possibility of signing contracts.

Also in this matter, an action from the regulatory body to ensure standardization would be able to take out these barriers.

## 5.3. The role of communication

A clear insight that emerged from the interview is how communication is key in obtaining a wide diffusion for digital identity solutions. Several managers, especially from the insurance and utility industries, have reported how in the first place SPID and CIE were perceived as solutions exclusively meant for the public sector. Targeted communication in these regards could greatly impact the perception of SPID and CIE among both firms and citizens, positively affecting their adoption by private SPs.

Firms-wise, the theme of communication is particularly relevant for those companies that do not require a high LOA. While banks are constantly monitoring digital identities both in the Italian and European scenarios, other industries pay less attention to the evolution of these solutions. For these reasons, especially as

long as SPID and CIE have not reached mass diffusion, pushing for firms to evaluate the possibility of adopting them is fundamental.

Communication might be the solution to some of the criticalities that are keeping CIE several steps behind SPID. Currently CIE is perceived as a substitutive solution of SPID, rather than complementary. Although being a minority, companies that are evaluating the adoption of CIE are interested in use-cases related to its NFC technology and in its validity as an identification document. These companies have a deep knowledge and understanding of the digital identity scenario, and are able to see the inner potentialities and capability of CIE. On the other side, the general perception around CIE is of a tool that carries the same capabilities of SPID but is enabled by a more complicated technology. Communication on alternative use-cases for CIE and on its ease of use could partially or totally fill the gap between the two solutions in exam.

# Bibliography

C. Allen (2016). "The path to self-sovereign identity." Available: http://www .coindesk.com

Anderson-Priddy and Toth (2019). "Self-Sovereign Digital Identity: A Paradigm Shift for Identity."

Lennart Ante, Constantin Fischer, Elias Strehle (2022). "A bibliometric review of research on digital identity: Research streams, influential works and future research paths."

BBVA (2018). *Digital Identity: the current state of affairs*.

[1] Ben Ayed, G. (2014). Architecting user-centric privacy-as-a-set-of-services. Cham: Springer International Publishing https://doi.org/10.1007/978-3-319-08231-8.

[2] Bertino E., Martino L., Paci F. and Squicciarini A. (2010). "Security for Web Services and Service- Oriented Architectures". Springer-Verlag Berlin Heidelberg.

Bouras M.A., Lu Q., Dhelim S. and Ning H. (2021) "A lightweight blockchain-based iot identity management approach", Future Internet, vol.13, pp. 1-14. Doi: 10.3390/fi13020024

Bromby M. (2010) "Identification, trust and privacy: How biometrics can aid certi.cation of digital signatures", International Review of Law, Computers and Technology, vol.24, pp. 133-141. Doi: 10.1080/13600861003644541

[3] Cameron, Posch and Rannenberg (2008). "A User-Centric Identity Metasystem".

[4] K. Cameron (2005). "The Laws of Identity," Microsoft Corpora- tion. 5 Nov. 2005.

[5] Cao F. and Cao Z. (2009). "A secure identity-based multi-proxy signature scheme". In: *Computers and Electrical Engineering*, vol.35, pp. 86-95. Doi: 10.1016/j.compeleceng.2008.05.005.

Y. Cao and L. Yang (2010). "A Survey of Identity Management Technology". In: *IEEE International Conference on Information Theory and Information Security*, Beijing, 17-19 December 2010, pp. 287-293. doi:10.1109/ICITIS.2010.5689468.

Chadwick, David W. (2009). "Federated Identity Management". Aldini, Alessandro and Barthe, Gilles and Gorrieri, Roberto, eds. FOSAD 2008/2009. LNCS (5705). Springer-Verlag, Berlin, pp. 182-196. ISBN 978-3-642-03828-0.

Dasgupta D., Roy A., Nag A. (2017). "Multi-Factor Authentication". In: *Advances in User Authentication* (pp.185-233).

De Angelis F., Falcioni D., Ippoliti F., Marcantoni F. and Rilli S. (2016). "Federated identity management in e-government: lessons learned and the path forward'. In: *International Journey Electronic Governance*, Vol. 8, No. 1, pp.22–38.

Dib O. and Toumi K. (2020). "Decentralized identity systems: Architecture, challenges, solutions and future directions". *Annals of Emerging Technologies in Computing*, vol.4, pp. 19-40. Doi: 10.33166/AETIC.2020.05.002.

Dunphy P. and Petitcolas F.A.P. (2018) "A first look at identity management schemes on the blockchain", IEEE Security and Privacy, vol.16, pp. 20-29. Doi: 10.1109/MSP.2018.3111247

Eisenhardt, Kathleen M and Melissa E Graebner (2007). "Theory building from cases: Opportunities and challenges". In: Academy of management journal 50.1, pp. 25–32.

European Commission (2020). *Business trends report – Bring Your Own Identity.*

Akmal F. Fainusa, Rahmat Nurcahyo, M. Dachyar (2019). "Conceptual Framework for Digital Wallet User Satisfaction."

Martha S. Feldman and Wanda J. Orlikowski (2011). "Theorizing Practice and Practicing Theory." In: OrganizationScience Vol. 22, No. 5, September–October 2011, pp. 1240–1253 issn 1047-7039 eissn 1526-5455 11 2205 1240108

Gartner (2019). *Innovation Insight for Bring Your Own Identity.*

Gioia, Dennis A, Kevin G Corley, and Aimee L Hamilton (2012). "Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. Organizational Research Methods".

Glaser, Barney G, Anselm L Strauss, and E Strutzel (1967). *TI, e discovery of grounded theory: Strategies for qualitative research*.

Md Arif Hassan, and Zarina Shukur (2020). "Review of Digital Wallet Requirements."

Seongho Hong and Heeyoul Kim (2020). "VaultPoint: A Blockchain-Based SSI Model that Complies with OAuth 2.0."

Jovanović B., Milenković I., Sretenović M.B. and Simić D. (2016). "Extending identity management system with multimodal biometric authentication". In: *Computer Science and Information Systems*, vol.13, pp. 313-334. Doi:10.2298/CSIS141030003J.

Koriat, Asher, Morris Goldsmith, and Ainat Pansky (2000). "Toward a psychology of memory accuracy". In: Annual review of psychology 51.1, pp. 481–537.

Lee Jong-Hyouk (2017). "BIDaaS: Blockchain Based ID As a Service"

Li, Jiang et al. (2017) "A Survey on the Security of Blockchain Systems."

Lim S.Y., Fotsing P.T., Almasri A., Musa O., Kiah M.L.M., Ang T.F. and Ismail R. (2018) "Blockchain technology the identity management and authentication service disruptor: A survey", International Journal on Advanced Science, Engineering and Information Technology, vol.8, pp. 1735-1745. Doi: 10.18517/ijaseit.8.4-2.6838

Martin, Jeffrey A and Kathleen M Eisenhardt (2010). "Rewiring: Cross-business-unit collaborations in multibusiness organizations". In: Academy of Management Journal 53.2, pp. 265–301.

McKinsey Global Institute (2016). *Digital finance for all: Powering inclusive growth in emerging economies.*

McKinsey Global Institute (2019). "Digital Identification: a key to inclusive growth".

Mohamed A. and Samion N.A. (2020). "Innovation of national digital identity: A review". In: *International Journal of Advanced Trends in Computer Science and Engineering*, vol.9, pp.151-159. Doi: 10.30534/IJATCSE/2020/2391.22020.

Nitin Naik and Paul Jenkins (2020). "Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology."

O'Gorman L. (2003) "Comparing passwords, tokens, and biometrics for user authentication", // Proceedings of the IEEE, 91, 12(2003), pp. 2021-2040. https://doi.org/10.1109/JPROC.2003.819611

Ometov and Bezzateev (2017). "Multi-factor Authentication: A Survey and Challenges in V2X Applications" presented at the 9th International Congress on Ultra Modern Telecommunications and Control Systems (ICUMT) on 6 November 2017.

Páez R., Pérez M., Ramírez G., Montes J. and Bouvarel L. (2020) "An architecture for biometric electronic identification document system based on blockchain", Future Internet, vol.12. Doi: 10.3390/fi12010010

Pöhn D. and Hommel W. (2020). "An Overview of Limitations and Approaches in Identity Management. In Proceedings of the 15th International Conference on Availability, Reliability and Security". Association for Computing Machinery, New York, NY, USA, Article 90, 1–10. DOI: https://doi.org/10.1145/3407023.3407026.

Prabhakar S., Ivanisov A. and Jain A. (2011) "Biometric recognition: Sensor characteristics and image quality", IEEE Instrumentation and Measurement Magazine, vol.14, pp. 10-16. Doi: 10.1109/MIM.2011.5773529

Rasouli H. and Valmohammadi C. (2019). "Proposing a conceptual framework for customer identity and access management: A qualitative approach". In: *Global Knowledge, Memory and Communication*, vol.69, pp. 94-116. Doi: 10.1108/GKMC-02-2019-0014.

Shah S.W. and Kanhere S.S. (2019). "Recent Trends in User Authentication - A Survey". In: *IEEE Access*, vol.7, pp. 112505-112519. Doi: 10.1109/ACCESS.2019.2932400.

Straus, Anselm L and BG Glaser (1967). The discovery of grounded theory: Strategies for qualitative research.

Sullivan C. (2013). "Digital identity, privacy and the right to identity in the United States of America". *Computer Law and Security Review*, vol.29, pp. 348-358. Doi: 10.1016/j.clsr.2013.05.011.

W3C VCWG (2018). "Verifiable Claims Working Group Frequently Asked Questions". Available at: https://w3c.github.io/webpayments-ig/VCTF/charter/faq.html.

Wayman J.L. (2008). "Biometrics in identity management systems". In: *IEEE Security and Privacy*, vol.6, pp. 30-37. Doi: 10.1109/MSP.2008.28.

Wilton, R. (2008). "Identity and privacy in the digital age". *International Journal Intellectual Property Management*, Vol. 2, No. 4, pp.411–428.

World Bank Group (2021). *ID4D & G2Px Annual Report 2021.*

World Bank Group, GSMA and Secure Identity Alliance (2016). *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*.

World Economic Forum (2016). *A Blueprint for Digital Identity.*

World Economic Forum (2018). *Identity in a Digital World. A new chapter in the social contract*. Available at: https://www.weforum.org/reports/identity-in-a-digital-world-a-new-chapter-in-the- social-contract.

Yin, Robert K (2003). "Case study research: design and methods,(3rd) Sage Publications". In: Thousand Oaks, California.

# List of Figures

# List of Tables

# Appendix

## Interviews questions

### Proprietary identity management system

**State of Art**

#### Onboarding

1) Is there a way to perform onboarding to access your company services?
2) What solutions did you implement to manage customer onboarding phase?
3) Are there any steps in which a face-to-face interaction or identification documents are needed?
4) What personal data, attributes and information do you gather in the identification phase? For what purposes?
5) In what phase of the recognition process you do have the necessity to exchange information with other private or public organizations?
6) What are your next expected investments on this matter?

#### Authentication

7) Does your company offer any services for which a form of customer authentication is needed?
8) What online services do you offer to your customers?
9) Is there the possibility to benefit from your services in a physical way? Are the online and physical fruition of services integrated?
10) What solutions did you implement to manage the recognition and authentication of the user?
11) What are the next investments you have in program to perform on this process?

**Strategic choices**

### Pros and cons

12) What are the reasons that pushed your company into adopting these solutions for the user recognition?
13) What barriers did you have to face in the adoption of these solutions and in the integration with your current systems?
14) [**if NO digital onboarding**] For what reasons it is not possible to acquire a new client through digital channels?
15) [**if NO online authentication**] For what reasons is not possible to create a personal area and access services of your firm through digital channels?
16) Did you decide to rely on third parties or to manage these activities internally?

### Costs and payment model

17) What are your cost items while managing customers digital identity? What is the average cost per user in the onboarding process? And for a single authentication?

**Business function management**

### Organizational model and decision-making process

18) What function oversee identity management on your company?
19) What are the skills of the people in this function?
20) Is there any cross-function cooperation on this matter?
21) What is the typical decision-making process related to the introduction of a new digital identity system?

### Cybersecurity and normative compliance

22) Inside your organization, who manages the digital identity of your customers, the protection of their data and their online account lifecycle?
23) What technological solutions did you implement to grant integrity, availability, and security in term of users' data?
24) What efforts did your company make to comply with national and international regulation?
25) What is the level of assurance needed to access and benefit of your services? How many and which of your authentication factors are necessary?

## External digital identity systems

26) Did you implement, or evaluate the possibility for the customer to either register or access through an external digital identity system? (e.g., social ID)
27) What are the main characteristics that condition the attractiveness of an external digital identity system for your company?

## National Digital Identity Systems (SPID or CIE)

**State of Art**

28) Did you consider the possibility of adopting national identity systems such as SPID or CIE?

**[Already adopting companies]**

29) What are the characteristics of SPID and/or CIE that pushed your company into adopting the system?
30) For which recognition phase do you use SPID and/or CIE?
31) After adopting these systems, have you kept using the proprietary identity system?
32) After the adoption of these systems, did you renovate the business functions overseeing the identity management process?
33) What kinds of benefits did you encounter after the adoption of these systems?
34) Did you have to face barriers for the adoption? Of what kind? Did you deal with them?
35) Do you think that your choice will impact other players of your market? Do you think that other companies are evaluating this alternative?

**[Not yet adopting companies, but willing to]**

36) What benefits do you expect to obtain adopting SPID and/or CIE?
37) What reasons held you back and what barriers did you encounter?

**[Not adopting companies, without willingness to do so]**

38) What are the reasons behind your choice of not adopting these systems? What barriers did you encounter?

**Future developments**

**[Companies who already adopted SPID/CIE or willing to do so]**

39) What future evolutions do you expect for these national digital identity systems? What functionalities and features you would like to see implemented to reach greater synergies and benefits?

**[Not adopting companies, without willingness to do so]**

40) What future evolutions of these systems would make your reconsider your choice of not adopting them?

**[all]**

41) What are the attributes gathered by your company in order to identify your clients that could be made interoperable to other firms willing to recognize your same client?
42) Recently it emerged the possibility to develop a communitarian digital identity, at an European level, integrated with current national digital identity systems. What do you think of this proposal? Does your company have any interest in integrating in a European ecosystem?

**Engagement strategies and payment modalities**

43) What are the business models (e.g., pay-per-use, subscription etc.) for the use of national digital identity systems that you think the best suits your needs?

# Acknowledgments

A conclusione di questo elaborato, vorrei ringraziare tutte le persone che mi hanno supportato nel raggiungimento di questo obiettivo.

Vorrei ringraziare il relatore di questo lavoro, il Professor Gastaldi, e Giorgia Dragoni, due persone a cui guardo come modelli e che stimo immensamente sia dal punto di vista umano che professionale.

Vorrei ringraziare Clarissa, per la professionalità, la pazienza, la gentilezza, la perseveranza, il supporto, l'empatia e la comprensione. Per rappresentare ciò che il Politecnico è e dovrebbe essere.

Grazie agli amici, chi c'era, chi c'è stato e chi ci sarà, vi voglio bene, ve ne vorrò sempre.

Desidero ringraziare la mia famiglia, che mi ha sempre sostenuto, nei momenti felici ma soprattutto in quelli bui, e che so continuerà a farlo per sempre. Spero di poter fare anche io la mia parte.

Grazie Nadia, per avermi supportato in tutti i modi in cui si può essere supportati. Mi dai il coraggio di dormire la sera e la forza di alzarmi la mattina. Questa tesi è anche tua.

Grazie a mia madrina, per avermi fatto sentire a casa.

Grazie a mio padre, per avermi sempre consigliato.

Grazie a Carlo, per avermi capito quando molti non capivano.

Ma soprattutto grazie a mia mamma, mia forza, mio motore, mio cuore. Grazie per sostenermi da quando sono nato, il tuo amore è un modello di vita.